Power Domain Constructions

Reinhold Heckmann

FB 14 – Informatik
Universität des Saarlandes
D-6600 Saarbrücken
Bundesrepublik Deutschland

email: heckmann@cs.uni-sb.de

September 10, 1998

Abstract

The variety of power domain constructions proposed in the literature is put into a general algebraic framework. *Power constructions* are considered algebras on a higher level: for every ground domain, there is a power domain whose algebraic structure is specified by means of axioms concerning the algebraic properties of the basic operations empty set, union, singleton, and extension of functions. A host of derived operations is introduced and investigated algebraically. Every power construction is shown to be equipped with a *characteristic semiring* such that the resulting power domains become semiring modules. *Power homomorphisms* are introduced as a means to relate different power constructions. They also allow to define the notion of *initial* and *final* constructions for a fixed characteristic semiring. Such initial and final constructions are shown to exist for every semiring, and their basic properties are derived. Finally, the known power constructions are put into the general framework of this paper.

1 Introduction

A power domain construction maps every domain $\mathbf{X}$ of some distinguished class of domains into a so-called power domain over $\mathbf{X}$ whose points represent sets of points of the ground domain. Power domain constructions were originally proposed to model the semantics of non-deterministic programming languages [14, 16, 10, 13]. Other motivations are the semantic representation of a set data type [9], or of relational data bases [2, 5].

In 1976, Plotkin [14] proposed the first power domain construction. Because his construction goes beyond the category of bounded complete algebraic domains, Plotkin proposed the larger category of *SFP-domains* that is closed under his construction. A short time later, Smyth [16] introduced a simpler construction, the upper or Smyth power construction, that respects bounded completeness. In [17], a third power domain construction occurs, the lower power domain, that completes the trio of classical power domain constructions.

Starting from problems in data base theory, Buneman et al. [2] proposed to combine lower and upper power domain to a so-called sandwich power domain. Gunter investigated the logic of the classical power domains [4]. By extending the logic of Plotkin's domain in a natural way, he developed a so-called mixed power domain [5, 6]. Plotkin's power domain is a subset of the mixed one, and this in turn is a subset of the sandwich power domain.

We independently found the sandwich and mixed power domains in an isomorphic form as big and small set domains when developing domain constructions that would give semantics to an abstract data type of sets in a functional programming language (see [9]).

Given at least five different power domain constructions, the question arises what is the essence of these constructions, i.e. what are their common features which allow the application of the notion 'power domain'. Thus, we look for a theory of power domain constructions that covers the existing ones and provides answers to the following questions:

(1) What are power domain constructions?

(2) How are different power domain constructions related to each other?

(3) Are there more than the five constructions enumerated above?

(4) If so, how are these five constructions distinguished among all the others?

In addition, a general theory of power constructions provides — if it is to be useful — general theorems that are applicable to all specific power domain constructions.

Gunter presents in [6] the semantics of a non-deterministic language in terms of a generic power domain construction using the three basic operators of singleton, binary union, and extending set-valued functions from points to sets. These generic semantics may then be instanciated by choosing a concrete construction instead of the generic one. The concrete construction only has to provide the necessary basic operations.

Thus, we define a power domain construction by axioms concerning the existence of some basic operations. In addition, we specify some axioms that should be satisfied by the basic operations. One might worry about the actual choice of these axioms, but we think that our choice is quite natural. This opinion is strengthened by the fact that our definition leads to a rich theory, covers the known power constructions, and allows to characterize them algebraically.

After introducing some notions and notations, we present the basic operations and their axioms in section 3. In section 4, we indicate a variety of consequences of these axioms. Main proposed in [13] to define power domains as free modules over semirings. In section 5, we show that our power constructions are equipped with a *characteristic semiring*, and the resulting power domains are (not necessarily free) modules w.r.t. this semiring.

Power homomorphisms are introduced in section 6 as a means to relate different power constructions. They also allow to define the notion of *initial* and *final* constructions for a given characteristic semiring. In sections 8 and 9, we prove that such initial and final constructions exist for every semiring, and we derive their basic properties. Since the concept of a semiring is very general, we thus obtain a host of power domain constructions. The concluding section 10 then puts the five known power constructions mentioned above into the general framework of this paper.

2 Notions and notations

Following the programme outlined above, the paper mainly uses algebraic techniques, e.g. equational reasoning. Only a minimum of domain theory is needed; it is collected in this section.

A *poset* (partially ordered set) $(P, \leq)$ is a set P together with a reflexive, antisymmetric, and transitive relation '$\leq$'. Most often, we identify the poset $\mathbf{P} = (P, \leq)$ with its carrier P. We refer to the standard notions of upper and lower bounds, bounded subsets, least upper bound (lub) denoted by '$\bigsqcup$', greatest lower bound (glb), directed set, directed complete poset (*domain*), monotonic and continuous function.[1] Hence, a domain is just a directed complete poset. It need not possess a least element.

A domain is *bounded complete* if every bounded subset has a lub, and it is *complete* if all subsets have lubs. A domain is *discrete* if $x \leq y$ implies $x = y$. There is a one-to-one correspondence between discrete domains and (unordered) sets.

The product of two sets A and B is denoted by $A \times B$, and similarly, the product of two domains $\mathbf{X}$ and $\mathbf{Y}$ is written $\mathbf{X} \times \mathbf{Y}$. The set of all functions from a set A to a set B is denoted by $A \to B$, whereas the domain of continuous functions from domain $\mathbf{X}$ to domain $\mathbf{Y}$ is written $[\mathbf{X} \to \mathbf{Y}]$. Consequently, $f : A \to B$ means f is just a function, whereas $f : [\mathbf{X} \to \mathbf{Y}]$ means f is continuous. Continuous functions are also called *morphisms*.

A point a in a domain $\mathbf{X}$ is *way-below* a point b, written $a \ll b$, iff for all directed sets $D \subseteq \mathbf{X}$ with $b \leq \bigsqcup D$, there is an element d in D such that $a \leq d$. The domain is *continuous* if for every point x, the set $\{a \mid a \ll x\}$ is directed and has lub x.

A point a in a domain $\mathbf{X}$ is *isolated* (or: *finite*) iff it is way-below itself. The set of all isolated points of $\mathbf{X}$ is called $\mathbf{X}^0$. A domain $\mathbf{X}$ is *algebraic* iff every point of $\mathbf{X}$ is the lub of a directed set of isolated points. The set $\mathbf{X}^0$ of all isolated points of $\mathbf{X}$ is called the *base*. Every algebraic domain is continuous.

Bifinite or *profinite* domains [3] are the limits of ω-chains of finite domains. Every bounded complete algebraic domain is bifinite, and every bifinite domain is algebraic. The function space of two bifinite domains is bifinite again, whereas the function space of two algebraic domains need not be algebraic.

Following [15], a functor in the category of domains and continuous functions is *locally continuous* if its functional part acts continuously on the function spaces. Such functors are continuous. Hence they map bifinite domains to bifinite domains if they map finite domains to finite domains.

3 Specification of power constructions

3.1 Constructions

A power construction is something like a function which applied to a domain $\mathbf{X}$ yields a new domain, the power domain over $\mathbf{X}$. It is not really a function since there is no *set* of all domains. There may be total constructions that are applicable to all domains, as well as partial constructions applicable to a special class of domains only.

[1] w.r.t. directed sets, not ascending sequences.

Definition 3.1 A *(domain) construction* $\mathcal{F} : \mathbf{X} \mapsto \mathcal{F}\mathbf{X}$ attaches a domain $\mathcal{F}\mathbf{X}$ to every domain $\mathbf{X}$ belonging to a distinguished class *def* $\mathcal{F}$. $\mathcal{F}$ is a *total* construction if *def* $\mathcal{F}$ is the class of all domains, otherwise a partial one.

A *power (domain) construction* $\mathcal{P}$ is a domain construction satisfying the axioms presented in the next paragraphs. $\mathcal{P}\mathbf{X}$ is called the *power domain* over the *ground domain* $\mathbf{X}$. The elements of (the carrier of) $\mathcal{P}\mathbf{X}$ are called *formal sets*.

If a power construction $\mathcal{P}$ is defined for a class $\mathrm{C} = \mathit{def}\ \mathcal{P}$, then the power domains $\mathcal{P}\mathbf{X}$ are not required to be in C again.

Often, a power domain cannot be realized concretely as a set of subsets of the ground domain. Hence the notion of formal sets in contrast to actual sets, i.e. the ordinary subsets of the ground domain. Formal set operations will be notationally distinguished from actual set operations by means of additional bars, e.g. $\uplus$ vs. $\cup$.

In the following, the symbol $\mathcal{P}$ denotes a generic partial power construction defined for a class $\mathrm{D} = \mathit{def}\ \mathcal{P}$ of domains. We immediately require the class D to contain the one-point-domain $\mathbf{1}$ because the power domain $\mathcal{P}\mathbf{1}$ plays an important algebraic role.

3.2 Empty set and finite union

As a first requirement, we want the power domain $\mathcal{P}\mathbf{X}$ to contain a formal empty set and to provide formal set union. Both the existence of an empty set and the axioms for union may be subject to discussions.

None of the original power domain constructions contained the empty set. However, they were sometimes extended by the empty set in later developments. For our work, the empty set is important and cannot be dispensed with.

Mathematical set theory suggests that union be commutative, associative, and idempotent. The last requirement turns out to be the least important one. For the sake of generality, we omit it as far as possible. Thus, the following results apply for 'multi-power' domain constructions as well.

For a (generalized) power construction $\mathcal{P}$, all power domains $\mathcal{P}\mathbf{X}$ have to be equipped with a commutative and associative operation $\uplus : [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$. In addition, there has to be a point θ in $\mathcal{P}\mathbf{X}$ which is the neutral element of union '$\uplus$'. If union is idempotent, it is a real power construction, and otherwise a multi-power construction.

3.3 Monoid domains

To have generally applicable notions, we define the algebra of domains with empty set and union in a more abstract setting.

Definition 3.2 (Monoid domains and additive maps)

A *monoid domain* (or simply monoid) $(M, +, 0)$ is a domain M together with an associative operation $+ : [M \times M \to M]$ and an element 0 of (the carrier of) M which is the neutral element of '+'.

The monoid is *commutative* iff '+' is.

A map $f : [X \to Y]$ between two monoids is *additive* iff it is a *monoid homomorphism*, i.e. $f(0_X) = 0_Y$ and $f(a + b) = fa + fb$ hold.

Many authors, including myself in previous papers, call the additive maps linear. However, the term 'linear' is more appropriate for the module homomorphisms introduced in section 5.1. In many common cases, including the usual power constructions, additivity and linearity coincide.

3.4 Singleton sets

Returning to the power construction, we next require a morphism which maps elements into singleton sets. We denote it by $\iota = \{\!|.|\!\} : [\mathbf{X} \to \mathcal{P}\mathbf{X}]$, $x \mapsto \{\!|x|\!\}$.

By means of the operations θ and $\uplus$, we may extend $\{\!|.|\!\}$ to finite sequences of ground domain points:

$$\{\!|x_1, \ldots, x_n|\!\} = \begin{cases} \{\!|x_1|\!\} \uplus \cdots \uplus \{\!|x_n|\!\} & \text{if } n > 0 \\ \theta & \text{if } n = 0 \end{cases}$$

Because of commutativity and associativity, one is free to permute the n arguments of $\{\!|x_1, \ldots, x_n|\!\}$. If union is idempotent, one additionally might delete and add multiple occurrences of elements. Thus $\{\!|.|\!\}$ becomes a mapping from finite actual sets to formal sets in this case.

3.5 Function extension

So far, we required the existence of singletons, empty set, and binary union. Singleton and union are not yet interrelated by axioms, and there are no axioms yet relating power domains over different ground domains. Both relationships are established by the extension functional. It takes a set-valued function defined on points of a ground domain and extends it to formal sets.

Definition 3.3 Let $\mathbf{X}$ be a domain in D and $\mathbf{Z}$ an arbitrary domain. A function $F : [\mathcal{P}\mathbf{X} \to \mathbf{Z}]$ is an *extension* of a function $f : [\mathbf{X} \to \mathbf{Z}]$ iff $F\{\!|x|\!\} = fx$ holds for all x in X, or equivalently iff $F \circ \iota = f$.

For every two domains $\mathbf{X}$ and $\mathbf{Y}$ in D, *ext* is a morphism mapping morphisms from $\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$ into morphisms from $\mathcal{P}\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$. For every $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, the extended function $\overline{f} = ext\, f$ should be an additive extension of f. These axioms imply $\overline{f}\,\{\!|x_1, \ldots, x_n|\!\} = fx_1 \uplus \cdots \uplus fx_n$ for $n > 0$.

$$\begin{tikzcd} \mathcal{P}\mathbf{X} \arrow[r, "\overline{f}"] & \mathcal{P}\mathbf{Y} \\ \mathbf{X} \arrow[u, "\iota"] \arrow[ur, "f"'] & \end{tikzcd}$$

We call the *ext* axioms indicated above primary axioms because their relevance is immediate. In addition, we require some 'secondary axioms' which will be stated below as (Si). (S1) and (S2) specify additivity in the functional argument. In the next section, power constructions are shown to be functors by means of (S3) and (S4).

- For all domains $\mathbf{X}$, $\mathbf{Y}$ in D, there is a morphism $ext = {}^{-} : [[\mathbf{X} \to \mathcal{P}\mathbf{Y}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]]$ with

(P1) $\overline{f}\,\theta = \theta$

(P2) $\overline{f}\,(A \uplus B) = (\overline{f}\,A) \uplus (\overline{f}\,B)$

(P3) $\overline{f}\,\{\!|x|\!\} = f x$ or: $\overline{f} \circ \iota = f$

Together, (P1) through (P3) mean $\overline{f}$ is an additive extension of f.

(S1) $ext\,(\lambda x.\,\theta)\,A = \theta$ or shortly $ext\,\underline{\theta} = \underline{\theta}$ where $\underline{\theta}$ denotes the constant function $\lambda x.\,\theta$.

(S2) $ext\,(\lambda x.\, fx \uplus gx)\,A = (ext\,f\,A) \uplus (ext\,g\,A)$.
Raising '$\uplus$' to functions, one may shortly write $\overline{f \uplus g} = \overline{f} \uplus \overline{g}$.

(S3) $ext\,(\lambda x.\,\{\!|x|\!\})\,A = A$ or: $\overline{\iota} = id$

(S4) For every two morphisms $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $g : [\mathbf{Y} \to \mathcal{P}\mathbf{Z}]$,

$$ext\,g\,(ext\,f\,A) = ext\,(\lambda a.\,ext\,g\,(f a))\,A$$

holds for all A in $\mathcal{P}\mathbf{X}$, or: $\overline{g} \circ \overline{f} = \overline{\overline{g} \circ f}$

$$\begin{tikzcd}
\mathcal{P}\mathbf{X} \arrow[r, "\overline{f}"] & \mathcal{P}\mathbf{Y} \arrow[r, "\overline{g}"] & \mathcal{P}\mathbf{Z} \\
\mathbf{X} \arrow[u, "\iota"] \arrow[ur, "f"'] & \mathbf{Y} \arrow[u, "\iota"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Note that we do not require $\overline{f}$ to be the only morphism satisfying (P1) through (P3) for given f. However, an important class of power constructions will have this property. For these constructions, (S1) through (S4) become provable (see section 8). That is why we call them secondary axioms.

3.6 Examples

Sets may be conceived as discrete domains, and all functions between discrete domains are continuous. Hence, ordinary power set formation is a partial power domain construction defined for discrete domains.

- $\mathcal{P}_{set}\,\mathbf{X} = \mathcal{P}\mathbf{X} = \{A \mid A \subseteq \mathbf{X}\}$ ordered discretely for discrete domains $\mathbf{X}$,
- $\theta = \emptyset$,
- $A \uplus B = A \cup B$,
- $\{\!|x|\!\} = \{x\}$,
- $ext\, f\, A = \bigcup_{a \in A} fa$.

Union is obviously commutative, associative, and the empty set is its neutral element. The axioms for extension read as follows:

(P1) $\bigcup_{a \in \emptyset} fa = \emptyset$ (P2) $\bigcup_{c \in A \cup B} fc \;=\; \bigcup_{a \in A} fa \cup \bigcup_{b \in B} fb$

(P3) $\bigcup_{x \in \{a\}} fx = fa$

(S1) $\bigcup_{a \in A} \emptyset = \emptyset$ (S2) $\bigcup_{a \in A} (fa \cup ga) \;=\; \bigcup_{a \in A} fa \cup \bigcup_{a \in A} ga$

(S3) $\bigcup_{a \in A} \{a\} = A$ (S4) $\bigcup\{gb \mid b \in \bigcup_{a \in A} fa\} = \bigcup_{a \in A} \bigcup_{b \in fa} gb$

All these equations hold, i.e. $\mathcal{P}_{set}$ is a power construction.

$ext\, f$ is not the only additive extension of f if $\mathbf{X}$ is infinite. Another additive extension of $f : \mathbf{X} \to \mathcal{P}_{set}\mathbf{Y}$ is $FA = \begin{cases} \bigcup_{a \in A} fa & \text{if } A \text{ is finite} \\ \mathbf{Y} & \text{otherwise} \end{cases}$

An extension functional defined in this manner would however violate axiom (S3).

The empty set and all singletons are finite, and finite unions of finite sets are finite. Hence, there is another power construction for sets:

$$\mathcal{P}_{fin}\,\mathbf{X} = \{A \subseteq \mathbf{X} \mid A \text{ is finite}\}$$

whose operations are the restrictions of the operations above. In this construction, every function $f : \mathbf{X} \to \mathcal{P}_{fin}\,\mathbf{Y}$ has a unique additive extension.

3.7 Summary

A power construction is a tuple (D, $\mathcal{P}$, θ, $\uplus$, ι, $^{-}$) where

- D is a class of domains;
- $\mathcal{P}$ maps domains belonging to class D into domains;
- $\theta = (\theta_X)_{X \in \mathrm{D}}$ with $\theta_X : \mathcal{P}X$
- $\uplus = (\uplus_X)_{X \in \mathrm{D}}$ with $\uplus_X : [\mathcal{P}X \times \mathcal{P}X \to \mathcal{P}X]$
- $\iota = (\iota_X)_{X \in \mathrm{D}}$ with $\iota_X : [X \to \mathcal{P}X]$
- $^{-} = (ext_{XY})_{X,Y \in \mathrm{D}}$ with $ext_{XY} : [[X \to \mathcal{P}Y] \to [\mathcal{P}X \to \mathcal{P}Y]]$

satisfying the axioms (domain indices are dropped!)

(C) $A \uplus B = B \uplus A$

(A) $A \uplus (B \uplus C) = (A \uplus B) \uplus C$

(N) $\theta \uplus A = A \uplus \theta = A$

(P1) $\overline{f}\,\theta = \theta$

(P2) $\overline{f}\,(A \uplus B) = (\overline{f}\,A) \uplus (\overline{f}\,B)$

(P3) $\overline{f} \circ \iota = f$

(S1) $\overline{\lambda x.\,\theta} = \lambda X.\,\theta$

(S2) $\overline{f \uplus g} = \overline{f} \uplus \overline{g}$ with '$\uplus$' raised to functions

(S3) $\overline{\iota} = id$

(S4) $\overline{g} \circ \overline{f} = \overline{\overline{g} \circ f}$

4 Derived operations in a power construction

The operations as specified above allow to derive many other operations with useful algebraic properties. We first consider some set operations including function mapping (4.1), big union (4.2), and Cartesian product (4.3). Function mapping turns the power construction into a locally continuous functor.

In section 4.4, we concentrate on the power domain $\mathcal{P}\mathbf{1}$ over the one-point-domain $\mathbf{1}$ and show that it incorporates the inherent logic of the power construction in its operations. In section 4.5, existential quantification $\mathcal{E}$ is introduced. Given a formal set and a predicate, $\mathcal{E}$ intuitively tells whether some member of the set satisfies the predicate. In section 9, $\mathcal{E}$ will be used to define power domain constructions in terms of second order predicates.

Elements of a power domain $\mathcal{P}\mathbf{X}$ may be multiplied by logical values, i.e. members of $\mathcal{P}\mathbf{1}$ (see section 4.6). Intuitively, multiplication of A by the logical value b results in the conditional *if b then A else* $\emptyset$. In case $\mathbf{X} = \mathbf{1}$, this operation induces a binary operation within $\mathcal{P}\mathbf{1}$. This operation may be interpreted as conjunction (section 4.7).

4.1 Mapping of functions over sets

Given a morphism $f : [\mathbf{X} \to \mathbf{Y}]$, it can be composed with the singleton operation to obtain $\iota \circ f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. The resulting set-valued function can be extended to set arguments. Thus, we obtain

$$map = \widehat{\ }:\ [[\mathbf{X} \to \mathbf{Y}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]] \qquad \widehat{f} = \overline{\iota \circ f}.$$

The primary and some secondary axioms of extension may be translated into corresponding properties of *map*.

(P1)' $\widehat{f}\,\theta = \theta$

(P2)' $\widehat{f}\,(A \uplus B) = (\widehat{f}\,A) \uplus (\widehat{f}\,B)$

(P3)' $\widehat{f} \circ \iota = \iota \circ f$ or: $\widehat{f}\,\{\!|x|\!\} = \{\!|fx|\!\}$

(S3)' $\widehat{id} = id$

(S4)' $\widehat{g} \circ \widehat{f} = \widehat{g \circ f}$

$$\begin{tikzcd}
\mathcal{P}\mathbf{X} \arrow[r, "\widehat{f}"] & \mathcal{P}\mathbf{Y} \\
\mathbf{X} \arrow[r, "f"] \arrow[u, "\iota"] & \mathbf{Y} \arrow[u, "\iota"']
\end{tikzcd}$$

Proof:

(P1)' $\widehat{f}\,\theta = \overline{\iota \circ f}\,(\theta) = \theta$ by (P1)

(P2)' immediately by (P2)

(P3)' $\widehat{f} \circ \iota = \overline{\iota \circ f} \circ \iota = \iota \circ f$ by (P3)

(S3)' $\widehat{id} = \overline{\iota \circ id} = \overline{\iota} = id$ by (S3)

(S4)' $\widehat{g} \circ \widehat{f} = \overline{\iota \circ g} \circ \overline{\iota \circ f} \stackrel{(S4)}{=} \overline{\overline{\iota \circ g} \circ \iota \circ f} \stackrel{(P3)}{=} \overline{\iota \circ g \circ f} = \widehat{g \circ f}$ $\square$

The properties (P1)' through (P3)' imply $\widehat{f}\,\{\!|x_1, \ldots, x_n|\!\} = \{\!|f x_1, \ldots, f x_n|\!\}$. The last two properties show that $\mathcal{P}$ becomes a functor by means of *map*. Since *map* is continuous when considered a second order function, this functor is locally continuous, whence every power construction sends bifinite domains to bifinite domains if it sends finite domains to finite domains (see section 2).

4.2 Big union

If $\mathbf{X}$ is in D such that $\mathcal{P}\mathbf{X}$ is back in D again, the identity $id : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$ may be extended to a morphism $U = \overline{id} : [\mathcal{P}(\mathcal{P}\mathbf{X}) \to \mathcal{P}\mathbf{X}]$. The axioms (P1) through (P3) of extension imply

$$\begin{tikzcd}
\mathcal{P}(\mathcal{P}\mathbf{X}) \arrow[dr, "U"] & \\
\mathcal{P}\mathbf{X} \arrow[u, "\iota"] \arrow[r, "id"'] & \mathcal{P}\mathbf{X}
\end{tikzcd}$$

(1) $U\,\theta = \theta$

(2) $U\,(A \uplus B) = U A \uplus U B$

(3) $U\,\{\!|S|\!\} = S$

whence $U\,\{\!|S_1, \ldots, S_n|\!\} = S_1 \uplus \cdots \uplus S_n$. Thus, U is a formal big union of formal sets of formal sets.

4.3 Double extension

Let $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ be three domains in D, and let $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$ be a binary operation written in infix notation. By double extension, one obtains

$$A \overrightarrow{\star} B = ext\ (\lambda a.\ ext\ (\lambda b.\ a \star b)\ B)\ A \quad \text{and} \quad A \overleftarrow{\star} B = ext\ (\lambda b.\ ext\ (\lambda a.\ a \star b)\ A)\ B$$

The results are two morphisms $\overrightarrow{\star}, \overleftarrow{\star} : [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{Y} \to \mathcal{P}\mathbf{Z}]$.

A power construction is *symmetric* iff $A \overrightarrow{\star} B = A \overleftarrow{\star} B$ holds for all $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ in D, A in $\mathcal{P}\mathbf{X}$, B in $\mathcal{P}\mathbf{Y}$, and $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$. Power constructions are not automatically symmetric. Later, we shall meet examples for this.

Our two sample power constructions for discrete domains — set of arbitrary subsets and set of finite subsets — are both symmetric because of

$$\bigcup_{a \in A} \bigcup_{b \in B} a \star b = \bigcup_{b \in B} \bigcup_{a \in A} a \star b$$

For two singletons, $\{\!|a|\!\} \overrightarrow{\star} \{\!|b|\!\} = \{\!|a|\!\} \overleftarrow{\star} \{\!|b|\!\} = a \star b$ may be shown using (P3) twice. Because of (P1) and (P2), '$\overrightarrow{\star}$' is obviously additive in its first argument:

$$\theta \overrightarrow{\star} B = \theta \qquad (A_1 \uplus A_2) \overrightarrow{\star} B = (A_1 \overrightarrow{\star} B) \uplus (A_2 \overrightarrow{\star} B)$$

For additivity in the second argument, (S1) and (S2) have to be employed in addition because B appears in the functional argument of the outer occurrence of *ext*. Thus, we get

$$A \overrightarrow{\star} \theta = \theta \qquad A \overrightarrow{\star} (B_1 \uplus B_2) = (A \overrightarrow{\star} B_1) \uplus (A \overrightarrow{\star} B_2)$$

'$\overleftarrow{\star}$' has the same properties; the proofs are however exchanged.

For formal finite sets, one then obtains

$$\begin{aligned}&\{\!|x_1, \ldots, x_n|\!\} \overrightarrow{\star} \{\!|y_1, \ldots, y_m|\!\} = \{\!|x_1, \ldots, x_n|\!\} \overleftarrow{\star} \{\!|y_1, \ldots, y_m|\!\} = \\ &\qquad \{\!|x_i \star y_j \mid 1 \le i \le n,\ 1 \le j \le m|\!\}\end{aligned}$$

using an obvious generalization of ZF notation to formal sets.

Cartesian product of formal sets is a special instance of double extension. If $\mathbf{X}$ and $\mathbf{Y}$ are in D such that $\mathbf{X} \times \mathbf{Y}$ is also in D, then

$$\begin{aligned}A \overrightarrow{\times} B &= \mathit{ext}\ (\lambda a.\ \mathit{ext}\ (\lambda b.\ \{\!|(a,b)|\!\})\ B)\ A \quad \text{and} \\ A \overleftarrow{\times} B &= \mathit{ext}\ (\lambda b.\ \mathit{ext}\ (\lambda a.\ \{\!|(a,b)|\!\})\ A)\ B\end{aligned}$$

are formal Cartesian products.

If the class D where the power construction is defined is closed w.r.t. Cartesian product, then symmetry may be defined in terms of formal Cartesian products because of the following proposition:

Proposition 4.1 Let $\mathbf{X}$ and $\mathbf{Y}$ be in D such that $\mathbf{X} \times \mathbf{Y}$ also is in D. Then for all $\mathbf{Z}$ in D and $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$, $A \overrightarrow{\star} B = \mathit{ext}\,(\star)\,(A \overrightarrow{\times} b)$ and $A \overleftarrow{\star} B = \mathit{ext}\,(\star)\,(A \overleftarrow{\times} b)$ hold.

Proof:

$$\begin{aligned}\mathit{ext}\,(\star)\,(A \overrightarrow{\times} B) &= \mathit{ext}\ (\star)\ (\mathit{ext}\ (\lambda a.\ \mathit{ext}\ (\lambda b.\ \{\!|(a,b)|\!\})\ B)\ A) \\ &\overset{(S4)}{=} \mathit{ext}\ (\lambda a.\ \mathit{ext}\ (\star)\ (\mathit{ext}\ (\lambda b.\ \{\!|(a,b)|\!\})\ B))\ A \\ &\overset{(S4)}{=} \mathit{ext}\ (\lambda a.\ \mathit{ext}\ (\lambda b.\ \mathit{ext}\ (\star)\ \{\!|(a,b)|\!\})\ B)\ A \\ &\overset{(P3)}{=} \mathit{ext}\ (\lambda a.\ \mathit{ext}\ (\lambda b.\ a \star b)\ B)\ A\end{aligned}$$

The statement about '$\overleftarrow{\star}$' and '$\overleftarrow{\times}$' is proved analogously. □

Corollary 4.2 Let $\mathcal{P}$ be a power construction such that $\mathrm{D} = \mathit{def}\,\mathcal{P}$ is closed w.r.t. product, i.e. $\mathbf{X}$, $\mathbf{Y}$ in D implies $\mathbf{X} \times \mathbf{Y}$ in D. Then $\mathcal{P}$ is symmetric iff for all $\mathbf{X}$, $\mathbf{Y}$ in D, A in $\mathcal{P}\mathbf{X}$, and B in $\mathcal{P}\mathbf{Y}$, $A \overrightarrow{\times} B = A \overleftarrow{\times} B$ holds.

4.4 The logic of power constructions

Each power construction is equipped with an inherent logic. In this section, we present the domain of logical values together with disjunction and existential quantification. The corresponding conjunction is defined in section 4.7.

The domain of logical values is obtained by interpreting the power domain $\mathcal{P}\mathbf{1}$ where $\mathbf{1} = \{\diamond\}$. It has at least two elements: θ and $\{\!|\diamond|\!\}$, and is equipped with the binary operation '$\uplus$'. We interpret θ as 'false' denoted by 0, $\{\!|\diamond|\!\}$ as 'true' denoted by 1, and '$\uplus$' as formal disjunction '+'. From the power axioms, one gets the following properties:

- '+' is commutative and associative.
- $0 + a = a + 0 = a$ for all a in $\mathcal{P}\mathbf{1}$.
- In case of a real power construction, one additionally has $a + a = a$ for all a in $\mathcal{P}\mathbf{1}$.

Table of values for a generalized power construction:

+	0	1
0	0	1
1	1	?

for a real power construction:

+	0	1
0	0	1
1	1	1

Further statements about $\mathcal{P}\mathbf{1}$ beyond the ones above are not possible for generic power constructions. In particular, one does not know whether there are further logical values besides 1 and 0, and $a + 1 = 1$ does not generally hold, even for real power constructions. There is no information about the relative order of 0 and 1; 0 might be below 1, above 1, or incomparable to 1.

The two power set constructions — set of arbitrary subsets and set of finite subsets — both have the same logic: $\mathcal{P}\mathbf{1}$ is $\{\emptyset, \{\diamond\}\}$ or $\{0, 1\}$ with ordinary disjunction.

4.5 Existential quantification

Extension $ext : [[\mathbf{X} \to \mathcal{P}\mathbf{Y}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]]$ is polymorphic over the domains $\mathbf{X}$ and $\mathbf{Y}$. In this section, we consider the special case $\mathbf{Y} = \mathbf{1}$; section 4.6 is concerned with $\mathbf{X} = \mathbf{1}$.

Extension to the one-point domain $ex : [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}]]$[2] may be logically interpreted along the lines of the previous section. It has the following properties:

(P1) $ex\ p\ \theta = 0$

(P2) $ex\ p\ (A \uplus B) = (ex\ p\ A) + (ex\ p\ B)$

(P3) $ex\ p\ \{\!|x|\!\} = p\ x$

(S1) $ex\ (\lambda x.\ 0)\ A = 0$

(S2) $ex\ (\lambda x.\ p\ x + q\ x)\ A = (ex\ p\ A) + (ex\ q\ A)$

(S4) $ex\ p\ (ext\ f\ A) = ex\ (\lambda a.\ ex\ p\ (f a))\ A$

$$\begin{tikzcd} \mathcal{P}\mathbf{X} \arrow[rr, "ex\ p"] & & \mathcal{P}\mathbf{1} \\ \mathbf{X} \arrow[u, "\iota"] \arrow[urr, "p"'] & & \end{tikzcd}$$

whence $ex\ f\ \{\!|x_1, \ldots, x_n|\!\} = f x_1 + \cdots + f x_n$. Thus, ex means existential quantification. It takes a predicate $p : [\mathbf{X} \to \mathcal{P}\mathbf{1}]$ and a formal set A and tells whether some member of A

[2]This morphism is called ex to distinguish it from the fully polymorphic ext.

satisfies p. (S4) then informally reads: There is x in $\bigcup_{a \in A} fa$ satisfying p iff there is a in A such that there is x in fa satisfying p.

Existential quantification may also be used to translate formal sets into second order predicates. For this end, we exchange the order of arguments of ex by uncurrying, twisting, and then currying again. The outcome is a morphism $\mathcal{E} : [\mathcal{P}\mathbf{X} \to [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to \mathcal{P}\mathbf{1}]]$ mapping formal sets into second order predicates. The properties of ex presented above translate easily into properties of $\mathcal{E}$:

(P1) $\mathcal{E}\, \theta = \lambda p.\, 0$

(P2) $\mathcal{E}\,(A \uplus B) = \lambda p.\, (\mathcal{E}\, A\, p) + (\mathcal{E}\, B\, p)$

(P3) $\mathcal{E}\, \{\!|x|\!\} = \lambda p.\, p\, x$

(S4) $\mathcal{E}\,(ext\, f\, A) = \lambda p.\, \mathcal{E}\, A\,(\lambda a.\, \mathcal{E}\,(fa)\, p)$

These results suggest to define a power construction for given domain $\mathcal{P}\mathbf{1}$ by (a slight variant of) $\mathcal{P}\mathbf{X} = [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to \mathcal{P}\mathbf{1}]$. This method to obtain power constructions will be presented and explored in section 9.

4.6 Multiplication by a logical value

In this section, we consider extension of a morphism with domain $\mathbf{1}$, i.e. the instance $ext : [[\mathbf{1} \to \mathcal{P}\mathbf{X}] \to [\mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{X}]]$. The function space $[\mathbf{1} \to \mathcal{P}\mathbf{X}]$ is isomorphic to $\mathcal{P}\mathbf{X}$. Thus, we get a morphism $[\mathcal{P}\mathbf{X} \to [\mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{X}]]$. Uncurrying and exchanging arguments leads to the 'product' $\cdot : [\mathcal{P}\mathbf{1} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$. The definition is $b \cdot S = ext\,(\lambda\diamond.\, S)\, b$. We call this product external since its left operand is not a member of $\mathcal{P}\mathbf{X}$. The axioms of ext imply the characteristic properties of the product.

Proposition 4.3

(P1$\cdot$)	$0 \cdot S = \theta$
(P2$\cdot$)	$(a+b) \cdot S = (a \cdot S) \uplus (b \cdot S)$
(P3$\cdot$)	$1 \cdot S = S$
(S1$\cdot$)	$b \cdot \theta = \theta$
(S2$\cdot$)	$b \cdot (S_1 \uplus S_2) = (b \cdot S_1) \uplus (b \cdot S_2)$
(S4$\cdot$)	$ext\, f\,(b \cdot S) = b \cdot (ext\, f\, S)$
(S4a$\cdot$)	$(a \cdot b) \cdot S = a \cdot (b \cdot S)$
(SY$\cdot$)	If $\mathcal{P}$ is symmetric, then $ext\,(\lambda x.\, b \cdot fx)\, S = b \cdot (ext\, f\, S)$

Algebraists will notice that these properties essentially are the axioms of left modules. This topic will be further explored in section 5.1.

Proof:

(P1$\cdot$)	$0 \cdot S \;=\; ext\,(\lambda\diamond.\, S)\,\theta \;=\; \theta$
(P2$\cdot$)	$(a+b) \cdot S \;=\; ext\,(\lambda\diamond.\, S)\,(a \uplus b)$ etc.
(P3$\cdot$)	$1 \cdot S \;=\; ext\,(\lambda\diamond.\, S)\,\{\!|\diamond|\!\} \;=\; (\lambda\diamond.\, S)\diamond \;=\; S$
(S1$\cdot$)	$b \cdot \theta \;=\; ext\,(\lambda\diamond.\, \theta)\, b \;=\; \theta$
(S2$\cdot$)	$b \cdot (S_1 \uplus S_2) \;=\; ext\,(\lambda\diamond.\, S_1 \uplus S_2)\, b$ etc.

$$
\begin{array}{llcl}
(\mathrm{S4}\cdot) & \mathit{ext}\, f\, (b \cdot S) & = & \mathit{ext}\, f\, (\mathit{ext}\, (\lambda\diamond.\, S)\, b) \\
 & (\mathrm{S4}): & = & \mathit{ext}\, (\lambda\diamond.\, \mathit{ext}\, f\, ((\lambda\diamond.\, S)\, \diamond))\, b \\
 & & = & \mathit{ext}\, (\lambda\diamond.\, \mathit{ext}\, f\, S)\, b \\
 & & = & b \cdot (\mathit{ext}\, f\, S)
\end{array}
$$

$$
\begin{array}{llcl}
(\mathrm{S4a}\cdot) & (a \cdot b) \cdot S & = & \mathit{ext}\, (\lambda\diamond.\, S)\, (a \cdot b) \\
 & (\mathrm{S4}\cdot): & = & a \cdot (\mathit{ext}\, (\lambda\diamond.\, S)\, b) \\
 & & = & a \cdot (b \cdot S)
\end{array}
$$

$$
\begin{array}{llcl}
(\mathrm{SY}\cdot) & \mathit{ext}\, (\lambda x.\, b \cdot f x)\, S & = & \mathit{ext}\, (\lambda x.\, \mathit{ext}\, (\lambda\diamond.\, f x)\, b)\, S \\
 & \text{by symmetry:} & = & \mathit{ext}\, (\lambda\diamond.\, \mathit{ext}\, (\lambda x.\, f x)\, S)\, b \\
 & & = & b \cdot (\mathit{ext}\, f\, S) \qquad \Box
\end{array}
$$

Interpreted logically, the product $b \cdot S$ resembles the conditional 'if b then S else θ'. At least for the cases $b = 1$ and $b = 0$, product and conditional coincide because of $1 \cdot S = S$ and $0 \cdot S = \theta$.

4.7 Conjunction

Up to now, the logical domain $\mathcal{P}\mathbf{1}$ was only equipped with constants 0 and 1 and a disjunction '+'. We now interpret the external product on $\mathcal{P}\mathbf{1}$ as conjunction since $a \cdot b$ resembles 'if a then b else θ'. The algebraic properties of conjunction $\cdot : [\mathcal{P}\mathbf{1} \times \mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{1}]$ are given by the next proposition:

Proposition 4.4

- $0 \cdot b = b \cdot 0 = 0$
- Distributivities: $\begin{array}{l}(a_1 + a_2) \cdot b = (a_1 \cdot b) + (a_2 \cdot b) \\ a \cdot (b_1 + b_2) = (a \cdot b_1) + (a \cdot b_2)\end{array}$
- Neutral element: $1 \cdot b = b \cdot 1 = b$
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- If the construction $\mathcal{P}$ is symmetric, then '$\cdot$' is commutative.

Proof:

- 0: immediate by (P1$\cdot$) and (S1$\cdot$)
- Distributivities: (P2$\cdot$) and (S2$\cdot$)
- 1: $1 \cdot b = b$ holds by (P3$\cdot$). $b \cdot 1 = \mathit{ext}\, (\lambda\diamond.\, \{\!|\diamond|\!\})\, b = b$ holds by (S3).
- Associativity is just (S4a$\cdot$).
- Commutativity: $a \cdot b = \mathit{ext}\, (\lambda\diamond.\, b)\, a = \mathit{ext}\, (\lambda\diamond.\, b \cdot 1)\, a =$ using (SY$\cdot$) $\Box$
  $b \cdot \mathit{ext}\, (\lambda\diamond.\, 1)\, a = b \cdot (a \cdot 1) = b \cdot a$

The axioms of generic power constructions do not allow to derive more algebraic properties for conjunction. In particular, idempotence of conjunction, the opposite distributivities, and the laws of absorption do not generally hold. On the other side, the existing laws are powerful enough to obtain the following table of values:

$\cdot$	0	1
0	0	0
1	0	1

5 Power constructions considered algebraically

5.1 Semirings and modules

The host of algebraic properties of power constructions may be described in terms of well-known algebraic structures.

Definition 5.1 (Semiring)
A semiring domain $(R, +, 0, \cdot, 1)$ is a domain R with continuous operations such that $(R, +, 0)$ is a commutative monoid, $(R, \cdot, 1)$ is a monoid, and multiplication '$\cdot$' is additive in both arguments, i.e.

$$a \cdot 0 = 0 \cdot a = 0 \qquad a \cdot (b_1 + b_2) = (a \cdot b_1) + (a \cdot b_2) \qquad (a_1 + a_2) \cdot b = (a_1 \cdot b) + (a_2 \cdot b)$$

The semiring is *commutative* iff its multiplication is, and it is *idempotent* iff its addition is, i.e. $a + a = a$ holds.

A semiring homomorphism $h : [R \to R']$ between two semirings is a mapping that preserves the semiring operations:

$$h\,(a + b) = h\,a + h\,b \qquad h\,(0) = 0' \qquad h\,(a \cdot b) = h\,a \cdot h\,b \qquad h\,(1) = 1'$$

The power domain $\mathcal{P}\mathbf{1}$ is such a semiring with $0 = \theta$, $a + b = a \uplus b$, $1 = \{\!|\diamond|\!\}$, and $a \cdot b = \mathit{ext}\,(\lambda\diamond.\,b)\,a$ as shown in the previous sections.

Semirings are generalizations of both rings and distributive lattices. These in turn are generalizations of fields and Boolean algebras. Hence, both the notations $(R, +, 0, \cdot, 1)$ as used in this paper and a more logical notation $(R, \vee, \mathsf{F}, \wedge, \mathsf{T})$ seem to be adequate.

When semiring domains are considered which are lattices, there is a high risk to confuse the order '$\leq$' of the domain and the lattice order '$\sqsubseteq$' defined by $a + b = b$. Generally, there is no relation between these two orders. In special cases only, they are equal or just opposite.

Definition 5.2 (Modules)
Let $R = (R, +, 0, \cdot, 1)$ be a semiring domain and $M = (M, +, 0)$ be a commutative monoid domain. $(R, M, \cdot)$ is a *module* iff

$$\begin{array}{ll} \cdot : [R \times M \to M] & \\ a \cdot 0_M = 0_M & a \cdot (B_1 + B_2) = (a \cdot B_1) + (a \cdot B_2) \\ 0_R \cdot A = 0_M & (a_1 + a_2) \cdot B = (a_1 \cdot B) + (a_2 \cdot B) \\ 1_R \cdot A = A & a \cdot (b \cdot C) = (a \cdot b) \cdot C \end{array}$$

We also say 'M is an R-module'.
Let M_1 and M_2 be two R-modules. A morphism $f : [M_1 \to M_2]$ is *linear* iff

$$f\,(A + B) = f\,A + f\,B \quad \text{and} \quad f\,(r \cdot A) = r \cdot f\,A$$

Particularly prominent modules are those over a field; they are called vector spaces. The notion of linearity is drawn from there.
The most important results of the previous sections may be summarized to

Theorem 5.3 Let $\mathcal{P}$ be a power construction and let

$$\begin{array}{ll} + = \uplus : & [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}] \\ 0 = \theta : & \mathcal{P}\mathbf{X} \\ \cdot = \lambda(a, S).\, ext\,(\lambda\diamond.\, S)\, a : & [\mathcal{P}\mathbf{1} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}] \\ 1 = \{\!|\diamond|\!\} : & \mathcal{P}\mathbf{1} \end{array}$$

Then $\mathcal{P}\mathbf{1}$ with these operations is a semiring domain, and $\mathcal{P}\mathbf{X}$ is a $\mathcal{P}\mathbf{1}$-module for all domains $\mathbf{X}$. For $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, the extension $\overline{f} : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ is linear, and $\overline{f} \circ \iota = f$ holds.

The semiring $\mathcal{P}\mathbf{1}$ is called the *characteristic semiring* of the power construction $\mathcal{P}$. Different power constructions may have the same characteristic semiring. For instance, the construction of the set of all subsets and the construction of the set of finite subsets for the class of discrete domains both have characteristic semiring $\{0, 1\}$ with $1 + 1 = 1$.

Conversely, one may wonder whether there is a power construction for every given semiring. The answer is yes; in sections 8 and 9, two distinguished constructions with given semiring are presented.

5.2 R-constructions

It is generally useful not to stick to the fact that the characteristic semiring be exactly $\mathcal{P}\mathbf{1}$. It is better to be more flexible and let the characteristic semiring be some isomorphic copy of $\mathcal{P}\mathbf{1}$. In this case, it is important to fix an isomorphism.

Definition 5.4 Let R be a semiring domain. An *R-construction* is a pair $(\mathcal{P}, \varphi)$ of a power construction $\mathcal{P}$ and a semiring isomorphism $\varphi : [R \to \mathcal{P}\mathbf{1}]$.

If R allows non-trivial automorphisms, then there are several different isomorphisms between $\mathcal{P}\mathbf{1}$ and R. Hence, we fix an isomorphism in the definition. The importance of this fixing will be seen in the subsequent sections. Nevertheless, we shall mostly use the sloppy notation '$\mathcal{P}$ is an R-construction' without explicitly mentioning the fixed isomorphism $\varphi : [R \to \mathcal{P}\mathbf{1}]$.

Various derived power operations involved the power domain $\mathcal{P}\mathbf{1}$ in their functionality. By means of the isomorphisms φ and φ^{-1}, they may be turned into operations involving R instead. For the sake of clarity, we mark the original operations by an asterisk in the following, and denote the original products by '$*$'.

$$\begin{array}{lll} \cdot : & [R \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}] & r \cdot A = \varphi r * A \\ ex : & [[\mathbf{X} \to R] \to [\mathcal{P}\mathbf{X} \to R]] & ex\, p = \varphi^{-1} \circ ex^*\,(\varphi \circ p) \\ \mathcal{E} : & [\mathcal{P}\mathbf{X} \to [[\mathbf{X} \to R] \to R]] & \mathcal{E} A\, p = \varphi^{-1}\,(\mathcal{E}^* A\,(\varphi \circ p)) \end{array}$$

These new operations enjoy the same algebraic properties as the original operations. The proofs may be performed by simple equational reasoning. In the sequel, we shall mostly use the new operations.

5.3 Examples for characteristic semirings

In this section, we informally present some examples for power constructions and their characteristic semirings.

- The lower power construction has characteristic semiring $\{0 < 1\}$ where $1 + 1 = 1$. In this logic, 0 is unstable because it may become 1 while the computation proceeds. Thus, 0 actually means 'don't know' since only positive answers are reliable.

- The upper power construction has the dual semiring $\{1 < 0\}$. Here, 1 is unstable and may change to 0 in the course of a computation. Only negative answers are reliable.

- The convex or Plotkin power construction has semiring $\{0, 1\}$ with $1 + 1 = 1$. The elements are not comparable, whence computations with logical result cannot proceed. They have immediately to decide whether the result is 1 or 0, and cannot change their 'opinion' afterwards.

  The constructions of the set of all subsets and of the set of finite subsets have the same characteristic semiring as Plotkin's construction. Indeed, the construction of finite subsets is just a special instance of Plotkin's.

The three examples above show the importance of the empty set in our algebraic theory. Without empty set resp. 0, all three semirings would collapse to $\{1\}$ and could not be distinguished.

- A power construction with a more reasonable logic should have the Boolean domain $\mathbf{B} = \{\perp, 0, 1\}$ as semiring. Such constructions are called set domain constructions in [9]. The interpretation of $\perp$ is 'I do not (yet) know'. Computations with logical results start in this state which may change to 0 or 1 if the computation proceeds.

  The sandwich power domain [2] or big set domain [9] and the mixed power domain [5, 6] or small set domain [9] both have characteristic semiring $\mathbf{B}$ with parallel conjunction and disjunction.

- Multi-power domains containing formal multi-sets should have the natural numbers as their semiring. There are many different ways how to arrange the naturals to form a semiring domain. They may be ordered ascending, descending, or discretely; special elements $\perp$ or ∞ may be added etc.

  The multi-power domain of [1] has semiring $\{0, 1 < 2 < \cdots < \infty\}$, i.e. 0 is incomparable as in Plotkin's construction whereas the remaining naturals form an ascending chain.

- In [13], *discrete probabilistic non-determinism* is modeled by a power construction with characteristic semiring $\mathbf{R}_0^\infty$ — the non-negative reals including infinity ordered as usual with ordinary addition and multiplication.

- In [13] again, *oracle non-determinism* is modeled by a construction whose semiring is the power set of a fixed set. The power set is ordered by inclusion '$\subseteq$', addition is union, and multiplication is intersection.

- A third construction in [13] models *ephemeral non-determinism*. Its semiring is the so-called tropical semiring $\mathbf{T} = (\{0 < 1 < 2 < \cdots < \infty\}, \sqcap, \infty, +, 0)$, i.e. addition in $\mathbf{T}$ is minimum, and multiplication in $\mathbf{T}$ is arithmetic addition.

6 Power homomorphisms

6.1 Definition

Homomorphisms between algebraic structures are mappings preserving all operations of these structures. Power constructions may be considered algebraic structures on a higher level. Thus, it is also possible and useful to define corresponding homomorphisms.

A power homomorphism $H : \mathcal{P} \dot{\rightarrow} \mathcal{Q}$ between two power constructions $\mathcal{P}$ and $\mathcal{Q}$ with $\mathit{def}\ \mathcal{P} \subseteq \mathit{def}\ \mathcal{Q}$ is a 'family' of morphisms $H = (H_{\mathbf{X}})_{\mathbf{X} \in \mathit{def}\ \mathcal{P}} : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ commuting over all power operations, i.e.

$$\begin{tikzcd}
\mathbf{X} \arrow[d, "\iota"'] \arrow[dr, "H \circ f"] & \\
\mathcal{Q}\mathbf{X} \arrow[r, "\overline{H \circ f}"] & \mathcal{Q}\mathbf{Y} \\
\mathcal{P}\mathbf{X} \arrow[u, "H"] \arrow[r, "\overline{f}"] & \mathcal{P}\mathbf{Y} \arrow[u, "H"'] \\
\mathbf{X} \arrow[u, "\iota"] \arrow[ur, "f"'] &
\end{tikzcd}$$

- The empty set in $\mathcal{P}\mathbf{X}$ is mapped to the empty set in $\mathcal{Q}\mathbf{X}$: $H\theta = \theta$.
- The image of a union is the union of the images: $H(A \uplus B) = (HA) \uplus (HB)$.
- Singletons in $\mathcal{P}\mathbf{X}$ are mapped to singletons in $\mathcal{Q}\mathbf{X}$: $H\{\!|x|\!\}_{\mathcal{P}} = \{\!|x|\!\}_{\mathcal{Q}}$, or: $H \circ \iota_{\mathcal{P}} = \iota_{\mathcal{Q}}$.
- Let $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. Then $H \circ f : [\mathbf{X} \to \mathcal{Q}\mathbf{Y}]$, and $\mathit{ext}_{\mathcal{Q}}\,(H \circ f)\,(HA) = H(\mathit{ext}_{\mathcal{P}}\,f\,A)$ has to hold for all A in $\mathcal{P}\mathbf{X}$. This axiom may also be written $\mathit{ext}_{\mathcal{Q}}(H \circ f) \circ H = H \circ (\mathit{ext}_{\mathcal{P}}\,f)$ (see the figure to the right).

Obviously, there is an identity power homomorphism $I : \mathcal{P} \dot{\rightarrow} \mathcal{P}$ where all morphisms $I_{\mathbf{X}}$ are identities. Furthermore, two power homomorphisms $G : \mathcal{P} \dot{\rightarrow} \mathcal{Q}$ and $H : \mathcal{Q} \dot{\rightarrow} \mathcal{R}$ may be composed 'pointwise', i.e. $(H \circ G)_{\mathbf{X}} = H_{\mathbf{X}} \circ G_{\mathbf{X}}$. It is easy to show that the outcome is again a power homomorphism $H \circ G : \mathcal{P} \dot{\rightarrow} \mathcal{R}$.

A power isomorphism between two constructions $\mathcal{P}$ and $\mathcal{Q}$ is a family of isomorphisms $H = H_{\mathbf{X}} : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ such that both $(H_{\mathbf{X}})_{\mathbf{X} \in \mathit{def}\ \mathcal{P}}$ and $(H_{\mathbf{X}}^{-1})_{\mathbf{X} \in \mathit{def}\ \mathcal{Q}}$ are power homomorphisms. Hence, two isomorphic constructions are defined for the same class of domains.

6.2 Some properties of power homomorphisms

Since power homomorphisms preserve all primary power operations, it is not surprising that they also preserve the derived operations.

Proposition 6.1 Let $H : \mathcal{P} \dot{\rightarrow} \mathcal{Q}$ be a power homomorphism.

(1) Let $f : [\mathbf{X} \to \mathbf{Y}]$. Then $H \circ (\mathit{map}_{\mathcal{P}} f) = (\mathit{map}_{\mathcal{Q}} f) \circ H : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{Y}]$ (see the figure).

(2) Let b be in $\mathcal{P}\mathbf{1}$ and S in $\mathcal{P}\mathbf{X}$. Then $H(b \cdot S) = Hb \cdot HS$.

(3) $H_{\mathbf{1}} : [\mathcal{P}\mathbf{1} \to \mathcal{Q}\mathbf{1}]$ is a semiring homomorphism.

$$
\begin{tikzcd}
\mathcal{Q}\mathbf{X} \arrow[rrr, "map_{\mathcal{Q}}\, f"] & & & \mathcal{Q}\mathbf{Y} \\
& \mathbf{X} \arrow[ul, "\iota"] \arrow[dl, "\iota"'] \arrow[r, "f"] & \mathbf{Y} \arrow[ur, "\iota"'] \arrow[dr, "\iota"] & \\
\mathcal{P}\mathbf{X} \arrow[uu, "H"] \arrow[rrr, "map_{\mathcal{P}}\, f"] & & & \mathcal{P}\mathbf{Y} \arrow[uu, "H"']
\end{tikzcd}
$$

In categorical terms, (1) means H is a natural transformation between the functors $\mathcal{P}$ and $\mathcal{Q}$.

Proof:

(1) $$\begin{aligned} H \circ (map_{\mathcal{P}}\, f) &= H \circ (ext_{\mathcal{P}}\, (\iota_{\mathcal{P}} \circ f)) \;=\; (ext_{\mathcal{Q}}\, (H \circ \iota_{\mathcal{P}} \circ f)) \circ H \\ &= (ext_{\mathcal{Q}}\, (\iota_{\mathcal{Q}} \circ f)) \circ H \;=\; (map_{\mathcal{Q}}\, f) \circ H \end{aligned}$$

(2) $H(b \cdot S) = H(ext\,(\lambda\diamond.\, S)\, b) = ext\,(\lambda\diamond.\, HS)\,(Hb) = (Hb)\cdot(HS)$

(3) $H_{\mathbf{1}}$ respects $+ = \uplus$, $0 = \theta$, and $1 = \{\!|\diamond|\!\}$ by the definition of power homomorphisms. It respects '$\cdot$' by (2). $\square$

6.3 Linear power homomorphisms

In the following, we want to compare power constructions with the same characteristic semiring by means of power homomorphisms. We use the notion of R-constructions $\mathcal{P}$ with a fixed isomorphism from R to $\mathcal{P}\mathbf{1}$ as introduced in section 5.2.

Definition 6.2 Let R be a semiring, and let $(\mathcal{P}, \varphi)$ and $(\mathcal{P}', \varphi')$ be two R-constructions. A power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is called *linear* iff the morphisms $H_{\mathbf{X}} : [\mathcal{P}\mathbf{X} \to \mathcal{P}'\mathbf{X}]$ are R-linear.

Linearity of the morphisms is not a matter of course. Prop. 6.1 (2) tells $H(b \cdot S) = Hb \cdot HS$ instead for b in $\mathcal{P}\mathbf{1}$. From this, it becomes evident that a power homomorphism is linear iff it acts on R as an identity.

Proposition 6.3 Let $(\mathcal{P}, \varphi)$ and $(\mathcal{P}', \varphi')$ be two R-constructions. A power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is linear iff the composition $\varphi'^{-1} \circ H_{\mathbf{1}} \circ \varphi : [R \to R]$ is the identity.

Proof: To be sufficiently distinctive, we denote the product with members of $\mathcal{P}\mathbf{1}$ and $\mathcal{P}'\mathbf{1}$ by '$*$' in this proof. $r \cdot A$ is then defined by $\varphi r * A$ resp. $\varphi' r * A$.

Let H be a linear power homomorphism. Then for all r in R,

$$\begin{aligned} \varphi'^{-1}(H_{\mathbf{1}}(\varphi r)) &= \varphi'^{-1}(H_{\mathbf{1}}(\varphi r * \{\!|\diamond|\!\})) && \{\!|\diamond|\!\} \text{ is neutral in } \mathcal{P}\mathbf{1} \\ &= \varphi'^{-1}(H_{\mathbf{1}}(r \cdot \{\!|\diamond|\!\})) && R\text{-product '}\cdot\text{' defined by } \varphi \\ &= \varphi'^{-1}(r \cdot H_{\mathbf{1}}\{\!|\diamond|\!\}) && H \text{ is } R\text{-linear} \\ &= \varphi'^{-1}(\varphi' r * \{\!|\diamond|\!\}') && H \text{ is power homomorphism} \\ &= \varphi'^{-1}(\varphi' r) \;=\; r \end{aligned}$$

Conversely,

$$H(r \cdot S) = H(\varphi r * S) = H(\varphi r) * HS = \varphi'^{-1}(H(\varphi r)) \cdot HS = r \cdot HS$$

holds applying the definition of '$\cdot$' in terms of '$*$'. □

Hence, if R allows non-trivial automorphisms there are non-linear power homomorphisms besides the linear ones.

6.4 Initial and final R-constructions

Initial and final power constructions are defined relative to the characteristic semiring by means of *linear* power homomorphisms. Without the assumption of linearity, their existence could not be guaranteed.

An R-construction $\mathcal{P}$ is initial if for all R-constructions $\mathcal{Q}$ there is exactly one linear power homomorphism $\mathcal{P} \dot{\to} \mathcal{Q}$. Finality is dual. The exact definitions however are more complex. To prevent a construction from being initial simply because it is almost undefined, we concentrate on total constructions defined for all domains.

Definition 6.4

A total R-construction $(\mathcal{P}, \varphi)$ is *initial* if for all total R-constructions $(\mathcal{Q}, \varphi')$ there is exactly one linear power homomorphism $H : (\mathcal{P}, \varphi) \dot{\to} (\mathcal{Q}, \varphi')$.

A total R-construction $(\mathcal{P}, \varphi)$ is *final* if for all R-constructions $(\mathcal{Q}, \varphi')$ there is exactly one linear power homomorphism $H : (\mathcal{Q}, \varphi') \dot{\to} (\mathcal{P}, \varphi)$.

These definitions imply the existence and uniqueness of initial and final R-constructions for every given semiring domain R, as pointed out in sections 8 and 9. If the definitions did not refer to *linear* power homomorphisms, there would be no initial and final constructions for semirings with non-trivial automorphisms.

Initial and final R-constructions have the usual properties found in algebra:

(1) If $\mathcal{P}$ is isomorphic to an initial (a final) R-construction $\mathcal{P}'$, then $\mathcal{P}$ is also an initial (a final) R-construction.

(2) For given semiring R, initial and final R-constructions are unique up to isomorphism.

The proofs of these properties are done by standard algebraic arguments — provided that 'isomorphic' is understood as isomorphic by a linear power isomorphism.

The main result is the following theorem:

Theorem 6.5 For every semiring R, initial and final R-constructions exist.

In section 8, we demonstrate the initial construction. Section 9 is then devoted to the final construction. Before introducing the initial construction, we first investigate the theory of R-$\mathbf{X}$-*modules* because the results of this theory are used when considering the initial construction.

7 R-X-Modules

Before introducing the initial and final R-constructions for a semiring R, we consider R-$\mathbf{X}$-*modules* in this section. R-$\mathbf{X}$-modules are R-modules together with a map from $\mathbf{X}$. Power domains are R-$\mathbf{X}$-modules by the singleton map. The theory of R-$\mathbf{X}$-modules allows to prove a host of theorems that are applied to the theory of power domain constructions in the next section.

7.1 Definitions

An R-$\mathbf{X}$-module is an R-module together with a mapping from $\mathbf{X}$ to it.

Definition 7.1 An R-$\mathbf{X}$-*module* $\mathbf{M}$ is a pair $\mathbf{M} = (M, \eta)$ of an R-module domain M and a morphism $\eta : [\mathbf{X} \to M]$.

A morphism $f : (M, \eta) \to (M', \eta')$ is R-$\mathbf{X}$-*linear* iff $f : [M \to M']$ is R-linear and $f \circ \eta = \eta'$, i.e. $f(\eta x) = \eta' x$ for all x in $\mathbf{X}$.

We already met examples for such R-$\mathbf{X}$-modules and R-$\mathbf{X}$-linear mappings. If $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is a linear power homomorphism between two R-constructions, then for every ground domain $\mathbf{X}$, the instance $H_{\mathbf{X}}$ is an R-$\mathbf{X}$-linear mapping between the two R-$\mathbf{X}$-modules $(\mathcal{P}\mathbf{X}, \iota_{\mathcal{P}})$ and $(\mathcal{Q}\mathbf{X}, \iota_{\mathcal{Q}})$. If $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, then the extension $ext\, f$ is R-$\mathbf{X}$-linear between the R-$\mathbf{X}$-modules $(\mathcal{P}\mathbf{X}, \iota)$ and $(\mathcal{P}\mathbf{Y}, f)$ since $ext\, f \circ \iota = f$. Thus, the R-$\mathbf{X}$-modules with R-$\mathbf{X}$-linear mappings provide a common abstraction of extension and power homomorphisms.

In the sequel, we need some more definitions.

Definition 7.2 Let $\mathbf{M} = (M, \eta)$ where $M = (M, +, 0, \cdot, 1)$ is an R-module. A subset S of (the carrier of) M is called an R-$\mathbf{X}$-*submodule* of $\mathbf{M}$ iff

(1) ηx is in S for all $x \in \mathbf{X}$, i.e. $\eta[\mathbf{X}] \subseteq S$.

(2) 0 is in S.

(3) If a and b are in S, then so is $a + b$.

(4) If a is in S, then $r \cdot a$ is in S for all $r \in R$.

(5) S is a *subdomain* of M, i.e. S is *directed closed* in M, i.e. if D is a directed subset of S, then the limit of D w.r.t. M is in S.

By definition, S may be assumed to be an R-$\mathbf{X}$-module again, and the natural inclusion map $e : S \to M$ is an R-$\mathbf{X}$-linear morphism.

It is easily verified that the intersection of a family of R-$\mathbf{X}$-submodules of a fixed R-$\mathbf{X}$-module is again an R-$\mathbf{X}$-submodule. Hence, the R-$\mathbf{X}$-submodules form a complete lattice, and there is a least R-$\mathbf{X}$-submodule for every given R-$\mathbf{X}$-module $\mathbf{M}$. We call it the *core* $\mathbf{M}^c$ of $\mathbf{M}$. The following theorem is a generalization of a theorem found in [12] for the case $R = \{0, 1\}$. It provides a more explicit description of the core.

Theorem 7.3
If $\mathbf{M} = (M, \eta)$ is an R-$\mathbf{X}$-module, then its core is given by $\mathbf{M}^c = \overline{\mathbf{M}^{\#}}$ where

$$\mathbf{M}^{\#} = \{r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n \mid n \in \mathbf{N}_0,\, r_i \in R,\, x_i \in \mathbf{X}\}$$

and $\overline{B}$ is the least directed closed superset of B.

The size of $\mathbf{M}^c$ is bounded by $|\mathbf{M}^c| \leq 2^{(|R|^{|\mathbf{X}|})}$.

The proof of the theorem is included as an appendix.

7.2 Reduced R-$\mathbf{X}$-modules

Definition 7.4 An R-$\mathbf{X}$-module is *reduced* iff it coincides with its core.

Equivalently, an R-$\mathbf{X}$-module is reduced iff it does not allow proper R-$\mathbf{X}$-submodules.

For every R-$\mathbf{X}$-module $\mathbf{M}$, the core $\mathbf{M}^c$ is reduced. Hence, every R-$\mathbf{X}$-module contains a reduced R-$\mathbf{X}$-submodule.

Reduced R-$\mathbf{X}$-modules enjoy many interesting properties listed in the sequel.

Lemma 7.5 Let $\mathbf{M} = (M, \eta)$ be a reduced R-$\mathbf{X}$-module, and M' an R-module. If $F, G : [M \to M']$ are two R-linear morphisms with $F(\eta x) \leq G(\eta x)$ for all $x \in \mathbf{X}$, then $F \leq G$ holds.

Proof: Let $S = \{a \in M \mid Fa \leq Ga\}$. S satisfies the properties of Def. 7.2 whence $S = M$ follows because $\mathbf{M}$ admits no proper R-$\mathbf{X}$-submodules. □

By anti-symmetry, one immediately gets:

Proposition 7.6 In Lemma 7.5, '$\leq$' may be replaced by '$=$':
Let $\mathbf{M} = (M, \eta)$ be a reduced R-$\mathbf{X}$-module, and M' an R-module. If $F, G : [M \to M']$ are two R-linear morphisms with $F \circ \eta = G \circ \eta$, then $F = G$ holds.

As a special instance of this proposition, one obtains:

Proposition 7.7 If $\mathbf{M}$ is a reduced R-$\mathbf{X}$-module, then there is at most one R-$\mathbf{X}$-linear mapping from $\mathbf{M}$ to any other R-$\mathbf{X}$-module $\mathbf{M}'$.

Finally, we consider existence of a least element.

Proposition 7.8 If the semiring R has a least element $\bot_R$ and $\mathbf{X}$ has a least element $\bot_{\mathbf{X}}$, then every reduced R-$\mathbf{X}$-module $\mathbf{M} = (M, \eta)$ has a least element, namely $\bot_R \cdot \eta(\bot_{\mathbf{X}})$.

Proof: Let $S = \{a \in M \mid a \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})\}$.

(1) Let $x \in \mathbf{X}$. Then $\eta x = 1 \cdot \eta x \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(2) $0 = 0 \cdot \eta(\bot_{\mathbf{X}}) \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(3) Let $a, b \in S$. Then $a + b \geq \bot_R \cdot \eta(\bot_{\mathbf{X}}) + \bot_R \cdot \eta(\bot_{\mathbf{X}}) = (\bot_R + \bot_R) \cdot \eta(\bot_{\mathbf{X}}) \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(4) For $r \in R$ and $a \in S$, $r \cdot a \geq r \cdot \bot_R \cdot \eta(\bot_{\mathbf{X}}) \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(5) S is obviously closed w.r.t. limits of directed sets in M.

Hence, S satisfies the conditions of Def. 7.2, whence $S = M$ holds. □

7.3 Free R-$\mathbf{X}$-modules

By Prop. 7.7, there is at most one R-$\mathbf{X}$-linear mapping from every reduced R-$\mathbf{X}$-module. In this section, we consider an even more special class of R-$\mathbf{X}$-modules.

Definition 7.9 An R-$\mathbf{X}$-module $\mathbf{F}$ is *free* iff for every R-$\mathbf{X}$-module $\mathbf{M}$, there is exactly one R-$\mathbf{X}$-linear morphism from $\mathbf{F}$ to $\mathbf{M}$.

The existence of free R-$\mathbf{X}$-modules is shown in section 7.4. For algebraic R and $\mathbf{X}$, a more explicit construction is provided in section 7.5. In this section, we study the properties of free R-$\mathbf{X}$-modules. By usual algebraic arguments, all free R-$\mathbf{X}$-modules are isomorphic to each other. Thus, we sometimes denote *the* free R-$\mathbf{X}$-module by $R \odot \mathbf{X}$.

Proposition 7.10 Every free R-$\mathbf{X}$-module is reduced.

Proof:
Let $\mathbf{F}$ be a free R-$\mathbf{X}$-module and S an R-$\mathbf{X}$-submodule of $\mathbf{F}$. We have to show $S = \mathbf{F}$.

The embedding $\epsilon : S \to \mathbf{F}$ is R-$\mathbf{X}$-linear since S is an R-$\mathbf{X}$-submodule. Since $\mathbf{F}$ is free, there is an R-$\mathbf{X}$-linear morphism $\zeta : [\mathbf{F} \to S]$. The composition $\epsilon \circ \zeta$ is R-$\mathbf{X}$-linear and maps $\mathbf{F}$ to itself as the identity does. By freedom, $\epsilon \circ \zeta = id$ holds. Hence, for every y in $\mathbf{F}$, $y = \epsilon(\zeta y) \in S$ holds. $\square$

If $\mathbf{F}$ is a free R-$\mathbf{X}$-module, then for every morphism $f : [\mathbf{X} \to M]$ from $\mathbf{X}$ to some R-module M, there is a unique R-$\mathbf{X}$-linear extension $\overline{f} : [\mathbf{F} \to (M, f)]$ to the R-$\mathbf{X}$-module (M, f). Thus, '$^{-}$' itself is a function from $[\mathbf{X} \to M]$ to $[\mathbf{F} \to M]$.

Theorem 7.11 If $\mathbf{F}$ is a free R-$\mathbf{X}$-module, then for every R-module M, the mapping $^{-} : [\mathbf{X} \to M] \to [\mathbf{F} \to M]$ as introduced above is continuous.

Proof: '$^{-}$' is monotonic by Lemma 7.5 telling that $f \le g$ implies $\overline{f} \le \overline{g}$.

Now, we show the continuity of '$^{-}$'. Let η be the morphism from $\mathbf{X}$ to $\mathbf{F}$. Let $\mathcal{D}$ be a directed set of morphisms from $\mathbf{X}$ to M, and let f be its limit. We have to show $\overline{f} = \bigsqcup_{d \in \mathcal{D}} \overline{d}$. The function on the right hand side is R-linear by continuity of '$+$' and '$\cdot$'. It maps ηx to $f x$ by continuity of application and $\overline{d}(\eta x) = d\, x$. By uniqueness, it thus equals $\overline{f}$. $\square$

In the special case $\mathbf{X} = \mathbf{1}$, R itself is a free R-$\mathbf{X}$-module:

Proposition 7.12 $(R, \lambda x.\, 1)$ is a free R-$\mathbf{1}$-module.

Proof: Let $\mathbf{M} = (M, \eta)$ be an R-$\mathbf{1}$-module. Let $f : [R \to M]$ be given by $f(r) = r \cdot \eta \diamond$. This mapping is R-linear because of the module axioms. For instance, $f(r \cdot r') = (r \cdot r') \cdot \eta \diamond = r \cdot (r' \cdot \eta \diamond) = r \cdot f(r')$ holds. f is R-$\mathbf{1}$-linear since $f((\lambda x.\, 1) \diamond) = f(1) = 1 \cdot \eta \diamond = \eta \diamond$.

Let F be an arbitrary R-$\mathbf{1}$-linear map from $(R, \lambda x.1)$ to $\mathbf{M}$. Then $F(r) = F(r \cdot 1) = r \cdot F(1) = r \cdot F((\lambda x.\, 1) \diamond) = r \cdot \eta \diamond = f(r)$ holds, i.e. f is unique. $\square$

7.4 Existence of free modules

In this section, we show the existence of the free R-$\mathbf{X}$-module for arbitrary semiring domains R and ground domains $\mathbf{X}$. The proof follows the lines of [12] who proved the existence of the free commutative idempotent monoid over $\mathbf{X}$. Hoofman used the categorical Freyd Adjoint Functor Theorem. We avoid its usage for the sake of a slightly more explicit construction. Our proof looks much simpler than that of Hoofman because we apply the notion of R-$\mathbf{X}$-modules.

We first construct the so-called solution set required by the Adjoint Functor Theorem. Instead of applying this theorem after verifying its remaining preconditions and thus obtaining the mere existence of the free module, we present a simple explicit construction based on the solution set.

The problem with the class of all R-$\mathbf{X}$-modules is that it is not a set. The problem is solved by providing a set of R-$\mathbf{X}$-modules $\{\mathbf{M}_i \mid i \in I\}$ that may be used as representatives for all R-$\mathbf{X}$-modules.

Let c be the cardinal number $2^{(|R|^{|\mathbf{X}|})}$, and let C be a set of cardinality c. From C, we construct the set

$$D = \bigcup_{A \subseteq C} \{A\} \times (A \times A \to 2) \times (A \times A \to A) \times A \times (R \times A \to A) \times (\mathbf{X} \to A)$$

where $2 = \{0, 1\}$. Next, let I be the set of all tuples $(A, \leq, +, 0, \cdot, f)$ in D such that $\mathbf{A} = (A, \leq)$ is a domain, $M = (\mathbf{A}, +, 0, \cdot)$ is an R-module domain, and $f : \mathbf{X} \to \mathbf{A}$ is continuous, i.e. (M, f) is an R-$\mathbf{X}$-module. By construction, I contains isomorphic copies of all R-$\mathbf{X}$-modules up to cardinality c. Indexing I by itself, we obtain a family $(\mathbf{M}_i)_{i \in I}$ of R-$\mathbf{X}$-modules.

Now let $\mathbf{M} = (M, f)$ be an arbitrary R-$\mathbf{X}$-module. Let $\mathbf{M}^c$ be the core of $\mathbf{M}$ and $e : [\mathbf{M}^c \to \mathbf{M}]$ the natural inclusion. Note that e is R-$\mathbf{X}$-linear.

By Th. 7.3, $|\mathbf{M}^c| \leq 2^{(|R|^{|\mathbf{X}|})} = c$ holds. Hence, there is an isomorphic copy $\mathbf{M}_i$ of $\mathbf{M}^c$ in I. Let $\varphi : [\mathbf{M}_i \to \mathbf{M}^c]$ be the R-$\mathbf{X}$-linear isomorphism between $\mathbf{M}_i$ and $\mathbf{M}^c$.

Given the 'solution set' $(\mathbf{M}_i)_{i \in I}$, it is now easy to construct the free module. Let $\mathbf{P} = \prod_{i \in I} \mathbf{M}_i$. The operations in $\mathbf{P}$ are defined as follows:

- $a \leq b$ iff $a_i \leq b_i$ for all i in I,
- $a + b = (a_i + b_i)_{i \in I}$,
- $r \cdot a = (r \cdot a_i)_{i \in I}$ for r in R,
- $\eta x = (\eta_i\, x)_{i \in I}$ for $x \in \mathbf{X}$.

It is not difficult to see that all these functions are continuous, and make $\mathbf{P}$ into an R-$\mathbf{X}$-module. The projections $\pi_i : [\mathbf{P} \to \mathbf{M}_i]$ are R-$\mathbf{X}$-linear.

Finally, let $\mathbf{F}$ be the core of $\mathbf{P}$. Then the inclusion $p : \mathbf{F} \to \mathbf{P}$ is R-$\mathbf{X}$-linear. Summarizing, we get for each R-$\mathbf{X}$-module $\mathbf{M}$ the following chain of R-$\mathbf{X}$-linear mappings for some i:

$$\mathbf{F} \xrightarrow{p} \mathbf{P} \xrightarrow{\pi_i} \mathbf{M}_i \xrightarrow{\varphi} \mathbf{M}^c \xrightarrow{e} \mathbf{M}$$

Thus, we get an R-$\mathbf{X}$-linear map f from $\mathbf{F}$ to every R-$\mathbf{X}$-module $\mathbf{M}$. f is unique since $\mathbf{F}$ is reduced (Prop. 7.6).

7.5 Free modules in the algebraic case

There seems to be no general explicit description of the free R-$\mathbf{X}$-module. However, an explicit construction is possible at least in the case of *structurally algebraic* semiring R and algebraic domain $\mathbf{X}$.

Definition 7.13 A semiring domain R is *structurally algebraic* if it is algebraic and its base R^0 contains 0 and 1 and is closed w.r.t. '+' and '·'.

Examples:

- Every finite and every discrete semiring domain R is structurally algebraic since $R^0 = R$ holds in these cases.
- $\mathbf{N}_0^\infty = \{0 < 1 < 2 < \cdots < \infty\}$ is structurally algebraic since sum and product of finite numbers are finite.
- The tropical semiring $\mathbf{T}$ is algebraic but not structurally algebraic since ∞ is the neutral element of its addition.
- The powerset of an infinite set X with union as addition and intersection as multiplication and ordered by inclusion is algebraic but not structurally algebraic since $1 = X$ is infinite.

The actual construction is roughly indicated. First, let $\widehat{X}$ be the set of all (not necessarily monotonic) functions from $\mathbf{X}^0$ to R^0 that yield non-zero results for a finite number of arguments only. These functions α stand for finite R^0-linear combinations over $\mathbf{X}^0$ where αx is the coefficient of x. Hence, addition, multiplication by a member of R^0, singleton, and extension have natural definitions for $\widehat{X}$. Here, the closure of R^0 w.r.t. the algebraic operations is needed.

Second, $\widehat{X}$ is equipped with the least pre-order '$\preceq$' making singleton, addition, and multiplication monotonic. Extended functions $\widehat{f}$ may also be proven to be monotonic by showing that the pre-order $\alpha \preceq' \beta$ iff $\widehat{f}\alpha \leq \widehat{f}\beta$ also makes singleton, addition, and multiplication monotonic. The free R-module over $\mathbf{X}$ is then the ideal completion of this pre-order $(\widehat{X}, \preceq)$.
This explicit construction allows to derive the following properties:

Theorem 7.14 If R is structurally algebraic and $\mathbf{X}$ is algebraic, then $R \odot \mathbf{X}$ is algebraic.

Theorem 7.15 Let R be a finite semiring. If $\mathbf{X}$ is finite or bifinite, then so is $R \odot \mathbf{X}$.

Theorem 7.16 If R and $\mathbf{X}$ are discrete, then so is $R \odot \mathbf{X}$.

It leaves open the following
Problem: What happens if R is algebraic without being structurally algebraic?

8 The initial R-construction

In this section, the existence of the initial R-construction for given semiring R is shown and its properties are studied. The idea to consider initial power constructions dates back to [10]. Hoofman [12] showed the existence of the initial construction for semiring $\{0, 1\}$. Main [13] then proposed initial constructions for some fancy semirings as indicated in section 5.3. In contrast to our work, he requires the singleton mapping to be strict without telling exactly why. Our singleton mappings are generally non-strict as indicated by Prop. 7.8 and 9.4. The singleton maps of mixed and sandwich power domain are also non-strict.

For every domain $\mathbf{X}$ and every semiring R, there is a free R-$\mathbf{X}$-module $R \odot \mathbf{X}$. The construction $\mathbf{X} \mapsto R \odot \mathbf{X}$ is the initial R-construction.

Theorem 8.1 Let R be a fixed semiring. The power construction $\mathcal{P}$ defined by $\mathcal{P}\mathbf{X} = R \odot \mathbf{X}$ is the initial R-construction. The construction is symmetric iff R is commutative. The a priori given external product of the modules $\mathcal{P}\mathbf{X}$ coincides with the external product derived from the power operations.

Proof: We first show that $\mathcal{P}$ is a power construction. Empty set and union are given by the module operations: $\theta = 0$ and $A \uplus B = A + B$. Singleton is the morphism $\eta : [\mathbf{X} \to R \odot \mathbf{X}]$, i.e. $\{|x|\} = \eta x$. For every $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, the extension $\mathit{ext}\, f$ is given by the unique R-$\mathbf{X}$-linear map from $R \odot \mathbf{X}$ to $(\mathcal{P}\mathbf{Y},\, f)$. Function ext is continuous by Theorem 7.11. We have to demonstrate that it satisfies the power axioms.

The primary axioms of extension are satisfied by definition of ext. The secondary axioms are consequences of the uniqueness of the extended map.

(S1) $\mathit{ext}\,(\lambda a.\, \theta) = \lambda A.\, \theta$

The function to the right is linear and maps singletons to $\theta = 0$. The function to the left behaves equally, whence they are equal.

(S2) $\mathit{ext}\,(\lambda x.\, fx \uplus g\, x) = \lambda A.\, \mathit{ext}\, f\, A \uplus \mathit{ext}\, g\, A$

Both functions are linear, and both map a singleton $\{|a|\}$ to $fa \uplus ga$. Note that commutativity of the addition in a module is required to prove the additivity of the function ρ to the right because $\rho(A \uplus B) = \overline{f}A + \overline{f}B + \overline{g}A + \overline{g}B$, whereas $\rho A \uplus \rho B = \overline{f}A + \overline{g}A + \overline{f}B + \overline{g}B$.

(S3) $\mathit{ext}\, \iota = \mathit{id}$

Again, both sides are linear and coincide on singletons since both map $\{|a|\}$ to $\{|a|\}$.

(S4) $\mathit{ext}\, g \circ \mathit{ext}\, f = \mathit{ext}\,(\mathit{ext}\, g \circ f)$

Once more, both sides are linear — the left hand side as composition of linear maps. They both map a singleton $\{|a|\}$ to $\mathit{ext}\, g\,(fa)$.

In case of commutative semiring R, symmetry of the construction is shown by the same kind of reasoning in two steps:

(1) $\mathit{ext}\,(\lambda x.\, r \cdot fx) \;=\; \lambda A.\, r \cdot \mathit{ext}\, f\, A$

(2) $\mathit{ext}\,(\lambda a.\, \mathit{ext}\,(\lambda b.\, a \star b)\; B) \;=\; \lambda A.\, \mathit{ext}\,(\lambda b.\, \mathit{ext}\,(\lambda a.\, a \star b)\; A)\; B$

Next, we have to show that the primarily given external product of the R-module $\mathcal{P}\mathbf{X}$ coincides with the derived external product of the power construction. The latter is denoted by '$*$' for the moment.

$$r * A \;=\; ext\,(\lambda\diamond.\,A)\,r \;=\; ext\,(\lambda\diamond.\,A)\,(r\cdot 1) \;=\; r\cdot ext\,(\lambda\diamond.\,A)\,(\eta\diamond) \;=\; r\cdot A$$

using the linearity of extended maps.

By Prop. 7.12, $\mathcal{P}\mathbf{1} = R \odot \mathbf{1} = R$ holds, i.e. $(\mathcal{P},\, id)$ is an R-construction. Let $(\mathcal{Q},\, \varphi)$ be another R-construction. We have to demonstrate the existence of a unique linear power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$.

For every domain $\mathbf{X}$, $\mathcal{Q}\mathbf{X}$ is an R-module, and there is a morphism $\iota_{\mathcal{Q}} : [\mathbf{X} \to \mathcal{Q}\mathbf{X}]$. Since $\mathcal{P}\mathbf{X}$ is the free R-$\mathbf{X}$-module, there is a (unique) R-linear morphism $H : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ with $H \circ \iota_{\mathcal{P}} = \iota_{\mathcal{Q}}$. By linearity, H is additive, i.e. $H\theta = \theta$ and $H(A \uplus B) = HA \uplus HB$ hold.

Next, $H \circ (ext\, f) = ext\,(H \circ f) \circ H$ has to be shown for $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. Since H and all extensions are linear, both sides are linear morphisms from $\mathcal{P}\mathbf{X}$ to $\mathcal{Q}\mathbf{Y}$. They coincide on singletons: $H\,(ext\, f\, \{\!|x|\!\}_{\mathcal{P}}) = H\,(fx)$ and $ext\,(H \circ f)\,(H\{\!|x|\!\}_{\mathcal{P}}) = ext\,(H \circ f)\,\{\!|x|\!\}_{\mathcal{Q}} = H(fx)$ hold. Since $\mathcal{P}\mathbf{X}$ is free and $\mathcal{Q}\mathbf{Y}$ is an R-module, both sides are equal.

Uniqueness of H is a simple consequence of the freedom of $\mathcal{P}\mathbf{X}$ for all $\mathbf{X}$. □

The theory of R-$\mathbf{X}$-modules gives us the following properties of the initial R-construction:

Theorem 8.2 Let R be a semiring and let $\mathcal{P}$ be the initial R-construction.

(1) If R has a least element, then $\mathcal{P}$ maps domains with least element into domains with least element (Prop. 7.8).

(2) If R is structurally algebraic, then $\mathcal{P}$ maps algebraic domains into algebraic ones (Th. 7.14).

(3) If R is finite, then $\mathcal{P}$ maps (bi)finite domains into (bi)finite domains (Th. 7.15).

(4) If R is discrete, then $\mathcal{P}$ maps discrete domains into discrete ones (Th. 7.16).

9 The final R-construction

9.1 The main theorem

In contrast to the initial R-construction, the final one may be explicitly constructed. As indicated in section 4.5, existential quantification leads to a mapping $\mathcal{E}$ from $\mathcal{P}\mathbf{X}$ to $[[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to \mathcal{P}\mathbf{1}]$ for every power construction $\mathcal{P}$. This suggests to define $\mathcal{P}\mathbf{X}$ as $[[\mathbf{X} \to R] \to R]$ if $R = \mathcal{P}\mathbf{1}$ is given. The equations in section 4.5 also indicate how to define the power operations.

One has to prove that these operations satisfy the axioms of section 3, and that the derived semiring $\mathcal{P}\mathbf{1}$ is isomorphic to the original semiring R. For proving the axioms, the outer, second order mappings have to be additive, and for proving the isomorphism between $\mathcal{P}\mathbf{1}$ and R, they even have to be *right linear*.

Functions in $[\mathbf{X} \to R]$ may be multiplied by members of R from the right by defining $f \cdot r = \lambda x.\,(fx) \cdot r$. They also may be added by defining $f + g = \lambda x.\, fx + g\,x$. A second order function $F : [[\mathbf{X} \to R] \to R]$ is *right linear* iff $F(f + g) = Ff + Fg$ and $F(f \cdot r) = Ff \cdot r$ hold. The set of all such functions is denoted by $[[\mathbf{X} \to R] \overset{rlin}{\to} R]$. Ordered as subset of $[[\mathbf{X} \to R] \to R]$, it becomes a domain because the lub of a directed set of right linear functions is right linear again by continuity of application, sum, and external product.

Theorem 9.1 The *final R-construction* is given by $(\mathcal{P}, \varphi)$ where $\mathcal{P}\mathbf{X} = \mathcal{P}^R_f\mathbf{X} = [[\mathbf{X} \to R] \overset{rlin}{\to} R]$ and the isomorphism $\varphi : [R \to \mathcal{P}\mathbf{1}]$ is defined by $\varphi(r) = \lambda g.\, r \cdot g\diamond$. Its inverse is $\psi(A) = A(\lambda\diamond.\, 1)$.

The basic power operations are defined by

- $\theta = \lambda g.\, 0$
- $A \uplus B = \lambda g.\, Ag + Bg$
- $\{\!|x|\!\} = \lambda g.\, gx$ for $x \in \mathbf{X}$.
- $ext\, f\, A = \lambda g.\, A\,(\lambda a.\, fag)$ for $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $A \in \mathcal{P}\mathbf{X}$.

To understand the definition of *ext*, note that a ranges over $\mathbf{X}$. Then a in $\mathbf{X}$ and $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ imply $fa \in \mathcal{P}\mathbf{Y} = [[\mathbf{Y} \to R] \overset{rlin}{\to} R]$. g ranges over $[\mathbf{Y} \to R]$, whence $fag \in R$ and $\lambda a.\, fag : [\mathbf{X} \to R]$. Thus, $A \in \mathcal{P}\mathbf{X} = [[\mathbf{X} \to R] \overset{rlin}{\to} R]$ implies $A\,(\lambda \ldots) \in R$.

The proof of the theorem proceeds in four steps: First, it is shown that the power operations defined above always create right linear maps when applied to such maps. Second, the validity of the power axioms is shown by λ-conversions. Third, an isomorphism between $\mathcal{P}\mathbf{1}$ and R is established. Fourth, the power construction $\mathcal{P}^R_f$ is demonstrated to be final.

The proof of the right linearity of the results of the operations is done by straight-forward equational reasoning. It is omitted here. The remaining three steps are handled in the next three sections.

9.2 Proof step 2: The power axioms

In this section, we prove the validity of the power axioms for the new construction.

By the definition $A \uplus B = \lambda g.\, Ag + Bg$, the operation '$\uplus$' trivially is commutative, associative, and has neutral element $\theta = \lambda g.\, 0$. The axioms of extension are less easy to prove. In this paper, we concentrate on (P3) that is simple, (S2) where additivity of the second order function is needed, and (S4) which is the most difficult. The other ones are shown similarly.

Def.: $\quad ext\, f\, A = \lambda p.\, A\,(\lambda a.\, fap)$

(P3) $\quad ext\, f\, \{\!|x|\!\} \;=\; \lambda p.\, \{\!|x|\!\}\,(\lambda a.\, fap) \;=\; \lambda p.\, (\lambda a.\, fap)\,x \;=\; \lambda p.\, fxp \;=\; fx$

(S2)
$$\begin{aligned} ext\,(f \uplus g)\,A &= \lambda p.\, A\,(\lambda a.\,(f \uplus g)\,a\,p) \;=\; \lambda p.\, A\,(\lambda a.\,(fa \uplus ga)\,p) \\ &= \lambda p.\, A\,(\lambda a.\, fap + gap) \qquad \text{using additivity of } A \text{ here} \\ &= \lambda p.\, A\,(\lambda a.\, fap) + A\,(\lambda a.\, gap) \;=\; ext\, f\, A \uplus ext\, g\, A \end{aligned}$$

(S4) The claim is $ext\, g \circ ext\, f = ext\,(ext\, g \circ f)$, or $ext\, g\,(ext\, f\, A) \;=\; ext\,(\lambda x.\, ext\, g\,(f x))\, A$

$$\begin{array}{lcl}
ext\, g\,(ext\, f\, A) & = & \lambda p.\,(ext\, f\, A)\,(\lambda b.\, gbp) \\
 & = & \lambda p.\,(\lambda q.\, A\,(\lambda a.\, faq))\,(\lambda b.\, gbp) \\
 & = & \lambda p.\, A\,(\lambda a.\, f\, a\,(\lambda b.\, gbp)) \\
ext\,(\lambda x.\, ext\, g\,(fx))\, A & = & \lambda p.\, A\,(\lambda a.\,(\lambda x.\, ext\, g\,(fx))\, a\, p) \\
 & = & \lambda p.\, A\,(\lambda a.\,(ext\, g\,(fa))\, p) \\
 & = & \lambda p.\, A\,(\lambda a.\,(\lambda q.\,(fa)\,(\lambda b.\, gbq))\, p) \\
 & = & \lambda p.\, A\,(\lambda a.\, f\, a\,(\lambda b.\, gbp))
\end{array}$$

9.3 Proof step 3: The characteristic semiring

In this section, we show the power domain $\mathcal{P}\mathbf{1}$ and the original semiring R to be isomorphic. To this end, we first consider how the semiring operations in $\mathcal{P}\mathbf{1}$ are defined.

- $\mathcal{P}\mathbf{1} \;=\; [[\mathbf{1} \to R] \stackrel{rlin}{\to} R]$
- $0 \;=\; \theta \;=\; \lambda p.\, 0$
- $A + B \;=\; A \uplus B \;=\; \lambda p.\, Ap + Bp$
- $1 \;=\; \{\!|\diamond|\!\} \;=\; \lambda p.\, p\diamond$
- $$\begin{array}{lcl} A \cdot B \;=\; ext\,(\lambda\diamond.\, B)\, A & = & \lambda p.\, A\,(\lambda a.\,(\lambda\diamond.\, B)\, a\, p) \\ & = & \lambda p.\, A\,(\lambda a.\, B\, p) \;=\; \lambda p.\, A\,(\lambda\diamond.\, B\, p) \end{array}$$

  For the last equality, note that a ranges over $\mathbf{1}$.

There is one obvious choice for a mapping $\psi : [\mathcal{P}\mathbf{1} \to R]$, namely $\psi A = A\,(\lambda\diamond.\, 1)$. This mapping is a semiring homomorphism:

- $\psi\,(0) \;=\; (\lambda p.\, 0)\,(\lambda\diamond.\, 1) \;=\; 0$
- $\psi\,(A + B) \;=\; (\lambda p.\, Ap + Bp)\,(\lambda\diamond.\, 1) \;=\; \psi A + \psi B$
- $\psi\,(1) \;=\; (\lambda p.\, p\diamond)\,(\lambda\diamond.\, 1) \;=\; (\lambda\diamond.\, 1)\diamond \;=\; 1$
- $$\begin{array}{lcll} \psi\,(A \cdot B) & = & (\lambda p.\, A\,(\lambda\diamond.\, Bp))\,(\lambda\diamond.\, 1) & \\ & = & A\,(\lambda\diamond.\, B\,(\lambda\diamond.\, 1)) & \\ & = & A\,(\lambda\diamond.\, \psi B) \;=\; A\,(\lambda\diamond.\, 1 \cdot \psi B) & \quad \text{use right linearity of } A \text{ now} \\ & = & A\,(\lambda\diamond.\, 1) \cdot \psi B \;=\; \psi A \cdot \psi B & \end{array}$$

As announced previously, right linearity of the second order functions in $\mathcal{P}\mathbf{X}$ is needed here. With left linearity, the result would be $\psi\,(A \cdot B) = \psi B \cdot \psi A$ instead.

The mapping ψ is shown to be an isomorphism by specifying its inverse. Let $\varphi : [R \to \mathcal{P}\mathbf{1}]$ be defined by $\varphi r = \lambda p.\, r \cdot p\diamond$. The second order mapping φr is right linear in p because

$$\begin{array}{l}
\varphi r\,(p + p') \;=\; r \cdot (p + p')\diamond \;=\; r \cdot (p\diamond + p'\diamond) \;=\; r \cdot p\diamond + r \cdot p'\diamond \;=\; \varphi r\,(p) + \varphi r\,(p') \\
\varphi r\,(p \cdot a) \;=\; r \cdot (p \cdot a)\diamond \;=\; r \cdot (p\diamond \cdot a) \;=\; (r \cdot p\diamond) \cdot a \;=\; \varphi r\,(p) \cdot a
\end{array}$$

φ is the inverse of ψ since

$$\begin{array}{rcl}
\psi\,(\varphi r) & = & (\lambda p.\, r \cdot p\,\diamond)\,(\lambda\diamond.\, 1) \;=\; r \cdot (\lambda\diamond.\, 1)\,\diamond \;=\; r \cdot 1 \;=\; r \\
\varphi\,(\psi A) & = & \lambda p.\, \psi A \cdot p\,\diamond \\
 & = & \lambda p.\, A\,(\lambda\diamond.\, 1) \cdot p\,\diamond \qquad \text{and by right linearity of } A \\
 & = & \lambda p.\, A\,(\lambda\diamond.\, 1 \cdot p\,\diamond) \\
 & = & \lambda p.\, A\,(\lambda\diamond.\, p\,\diamond) \;=\; \lambda p.\, Ap \;=\; A
\end{array}$$

9.4 Proof step 4: Finality

Let $(\mathcal{Q},\, \rho)$ be an arbitrary R-construction and let $(\mathcal{P},\, \varphi)$ be the R-construction of Th. 9.1. We have to construct a linear power homomorphism $H : \mathcal{Q} \dot{\rightarrow} \mathcal{P}$ and then show it is unique. H is given by existential quantification $\mathcal{E} : [\mathcal{Q}\mathbf{X} \to [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]]$ as defined in section 5.2.

Existential quantification in $\mathcal{Q}$ would map functions in $[\mathbf{X} \to \mathcal{Q}\mathbf{1}]$ into elements of $\mathcal{Q}\mathbf{1}$. It can be used to define H if semiring elements can be translated into elements of $\mathcal{Q}\mathbf{1}$ and vice versa by means of ρ and ρ^{-1}. Hence we define for A in $\mathcal{Q}\mathbf{X}$

$$H\,A = \lambda p.\, \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,A)$$

Here, p ranges over $[\mathbf{X} \to R]$, whence $\rho \circ p : [\mathbf{X} \to \mathcal{Q}\mathbf{1}]$. Thus, $(ext_{\mathcal{Q}}\,(\rho \circ p)\,A)$ is in $\mathcal{Q}\mathbf{1}$, whence its value by ρ^{-1} is in R. Hence, $H : [\mathcal{Q}\mathbf{X} \to [[\mathbf{X} \to R] \to R]]$.

Adopting this definition of H, we have to show that $H\,A$ is right linear, that H is a linear power homomorphism, and finally that H is unique. We omit the proof of right linearity here immediately going on to the power homomorphism proof. Here, empty set and union are also omitted.

- $$H\,\{\!|x|\!\}_{\mathcal{Q}} \;=\; \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,\{\!|x|\!\}_{\mathcal{Q}}) \;\stackrel{(P3)}{=}\; \lambda p.\, \rho^{-1}\,(\rho\,(p\,x)) \;=\; \lambda p.\, p\,x \;=\; \{\!|x|\!\}_{\mathcal{P}}$$
- $$\begin{array}{rcl}
H\,(ext\,f\,A) & = & \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,(ext\,f\,A)) \\
 & \stackrel{(S4)}{=} & \lambda p.\, \rho^{-1}\,(ext\,(\lambda x.\, ext\,(\rho \circ p)\,(f\,x))\,A) \\
 & = & \lambda p.\, \rho^{-1}\,(ext\,(\lambda x.\, \rho\,(\rho^{-1}\,(ext\,(\rho \circ p)\,(f\,x))))\,A) \\
 & = & \lambda p.\, \rho^{-1}\,(ext\,(\lambda x.\, \rho\,(H\,(f\,x)\,p))\,A) \\
 & = & \lambda p.\, H\,A\,(\lambda x.\, H\,(f\,x)\,p) \\
 & = & \lambda p.\, H\,A\,(\lambda x.\, (H \circ f)\,x\,p) \\
 & = & ext_{\mathcal{P}}\,(H \circ f)\,(H\,A)
\end{array}$$

Now we know H is a power homomorphism. To show its linearity, we have to prove $\psi\,(H_{\mathbf{1}}\,(\rho r)) = r$ for all $r \in R$ by Prop. 6.3 where $\psi = \lambda S.\, S\,(\lambda\diamond.\, 1)$ is the isomorphism from $\mathcal{P}\mathbf{1}$ to R.

$$\begin{array}{rcl}
\psi\,(H_{\mathbf{1}}\,(\rho r)) & = & (\lambda p.\, \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,(\rho r)))\,(\lambda\diamond.\, 1) \\
 & = & \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ (\lambda\diamond.\, 1))\,(\rho r)) \\
 & = & \rho^{-1}\,(ext_{\mathcal{Q}}\,(\lambda\diamond.\, \{\!|\diamond|\!\}_{\mathcal{Q}})\,(\rho r)) \qquad \text{since } \rho\,(1) = \{\!|\diamond|\!\}_{\mathcal{Q}} \\
 & \stackrel{(S3)}{=} & \rho^{-1}\,(\rho r) \;=\; r
\end{array}$$

The last property to be shown is that H is the only linear power homomorphism from $\mathcal{Q}$ to $\mathcal{P}$. Let G be another linear power homomorphism. Then $\psi \circ G_{\mathbf{1}} \circ \rho = id_R$ holds.

$$
\begin{array}{rcll}
HA & = & \lambda p.\, \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,A) & \\
 & = & \lambda p.\, \psi\,(G_{\mathbf{1}}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,A)) & \text{since } \rho^{-1} = \psi \circ G_{\mathbf{1}} \\
 & = & \lambda p.\, \psi\,(ext_{\mathcal{P}}\,(G_{\mathbf{1}} \circ \rho \circ p)\,(GA)) & \text{because } G \text{ is a power homomorphism} \\
 & = & \lambda p.\, (ext_{\mathcal{P}}\,(\psi^{-1} \circ p)\,(GA))\,(\lambda\diamond.\,1) & \text{since } G_{\mathbf{1}} \circ \rho = \psi^{-1}, \text{ and } \psi S = S\,(\lambda\diamond.\,1) \\
 & = & \lambda p.\, (GA)\,(\lambda x.\,(\psi^{-1} \circ p)\,x\,(\lambda\diamond.\,1)) & \text{by definition of } ext_{\mathcal{P}} \\
 & = & \lambda p.\, (GA)\,(\lambda x.\,\psi\,(\psi^{-1}\,(p\,x))) & \text{since } S(\lambda\diamond.\,1) = \psi S \\
 & = & \lambda p.\, GA\,(\lambda x.\,p\,x) \; = \; \lambda p.\, GA\,p \; = \; GA &
\end{array}
$$

Now, the theorem is completely proved.

9.5 Derived operations

The definition of the final R-construction provides realizations for the principal power operations in terms of higher order functions. The derived operations may also be expressed in functional form.

- $$
\begin{array}{rcl}
map\, f\, A & = & ext\,(\iota \circ f)\,A \; = \; \lambda p.\, A\,(\lambda a.\,(\iota \circ f)\,a\,p) \\
 & = & \lambda p.\, A\,(\lambda a.\,\{\!|fa|\!\}\,p) \; = \; \lambda p.\, A\,(\lambda a.\,p\,(fa)) \; = \; \lambda p.\, A\,(p \circ f)
\end{array}
$$

- As indicated in section 5.2, the external product is defined for elements of R by means of φ.

$$
\begin{array}{rcl}
r \cdot A & = & ext\,(\lambda\diamond.\,A)\,(\varphi r) \; = \; \lambda p.\,(\varphi r)\,(\lambda a.\,(\lambda\diamond.\,A)\,a\,p) \\
 & = & \lambda p.\,(\lambda q.\, r \cdot q\,\diamond)\,(\lambda a.\,Ap) \; = \; \lambda p.\, r \cdot (\lambda a.\,Ap)\,\diamond \; = \; \lambda p.\, r \cdot Ap
\end{array}
$$

9.6 Further properties

This section is a collection of some simple properties of the final construction.

Proposition 9.2 If R is discrete, then $\mathcal{P}^R_f\mathbf{X}$ is discrete for all domains $\mathbf{X}$.

Proof: $\mathcal{P}^R_f\mathbf{X}$ is $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$ ordered pointwise, i.e. $A \leq B$ iff $Ap \leq Bp$ in R for all $p : [\mathbf{X} \to R]$. □

Proposition 9.3 If R is finite, then $\mathcal{P}^R_f\mathbf{X}$ is finite or bifinite whenever $\mathbf{X}$ is.

Proof: If R and $\mathbf{X}$ are finite, then so is $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$. According to section 2, $\mathcal{P}^R_f$ then maps bifinite domains into bifinite domains since it is a locally continuous functor. □

Problem: If R and $\mathbf{X}$ are bifinite (R not necessarily being finite), is $\mathcal{P}^R_f\mathbf{X}$ bifinite?

Problem: If R and $\mathbf{X}$ are algebraic, is $\mathcal{P}^R_f\mathbf{X}$ algebraic?

Proposition 9.4 If R and $\mathbf{X}$ have least elements $\perp_R$ and $\perp_{\mathbf{X}}$, then $\mathcal{P}^R_f\mathbf{X}$ has a least element, namely $\perp_R \cdot \{\!|\perp_{\mathbf{X}}|\!\}$.

Proof: We have to show $Ap \geq (\perp_R \cdot \{\!|\perp_{\mathbf{X}}|\!\})\,p$ for all $A : [[X \to R] \overset{rlin}{\to} R]$ and all $p : [X \to R]$.

$$\begin{aligned} Ap &= A(\lambda x.\, p\,x) \geq A(\lambda x.\, p(\perp_{\mathbf{X}})) \\ &= A(\lambda x.\, 1 \cdot p(\perp_{\mathbf{X}})) \overset{\text{rlin}}{=} A(\lambda x.\, 1) \cdot p(\perp_{\mathbf{X}}) \\ &\geq \perp_R \cdot p(\perp_{\mathbf{X}}) = \perp_R \cdot \{\!|\perp_{\mathbf{X}}|\!\}\, p = (\perp_R \cdot \{\!|\perp_{\mathbf{X}}|\!\})\,p \qquad \Box \end{aligned}$$

Problem: Is $\mathcal{P}_f^R$ symmetric whenever R is commutative?

Simple equational reasoning does not help here.

10 Known power constructions

In this section, we briefly consider how the known power constructions fit into the general framework. Most proofs are omitted since this topic will be subject of a different paper and may also be found in [8].

10.1 Lower power constructions

Let $\mathbf{L} = \{0 < 1\}$ with $1 + 1 = 1$ be the *lower semiring*. $\mathbf{L}$-modules are just those commutative monoids $(M, +, 0)$ with $a + a = a$ and $0 \leq a$ for all a in M. One easily verifies that in such monoids, $a + b$ is the least upper bound of a and b. Hence, $\mathbf{L}$-modules are just complete domains with sum being least upper bound and 0 being $\perp$.

Lower power constructions are the power constructions with characteristic semiring $\mathbf{L}$.

Theorem 10.1 Initial and final lower power construction are isomorphic. They are explicitly given by

(1) $\mathcal{L}\mathbf{X} = \{C \subseteq \mathbf{X} \mid C \text{ is Scott closed}\}$ ordered by inclusion '$\subseteq$',

(2) $\bigsqcup_{i \in I} A_i = \mathsf{cl} \bigcup_{i \in I} A_i$ where 'cl' denotes Scott closure,

(3) $\theta = \emptyset$,

(4) $A \uplus B = A \cup B$,

(5) $\{\!|x|\!\} = \downarrow x$,

(6) for arbitrary $\mathbf{L}$-modules M and morphisms $f : [\mathbf{X} \to M]$, the unique linear extension $\overline{f} : [\mathcal{L}\mathbf{X} \to M]$ is given by $\overline{f}C = \bigsqcup f[C]$.

We do not include the proof of this theorem here because it is a bit out of the scope of this paper and uses some topological techniques not introduced here.

10.2 Upper power constructions

Let $\mathbf{U} = \{1 < 0\}$ with $1 + 1 = 1$ be the *upper semiring*. $\mathbf{U}$-modules are just those commutative monoids $(M, +, 0)$ with $a + a = a$ and $a \leq 0$ for all a in M. One easily verifies that in such monoids, $a + b$ is the greatest lower bound of a and b. Hence, $\mathbf{U}$-modules are just domains with a continuous binary greatest lower bound and a top element.

Although $\mathbf{U}$ is just dual to $\mathbf{L}$, the situation is much more complex here. The reason is that in $\mathbf{L}$-modules, binary lub and directed lub well cooperate and imply the existence of all lubs and all glbs. In $\mathbf{U}$-modules however, binary lubs and infinite glbs need not exist. The additional complexity might be the reason that the following theorem is much weaker than Th. 10.1.

Theorem 10.2 For continuous ground domain $\mathbf{X}$, the initial upper power domain $\mathcal{U}_i\mathbf{X}$ and the final upper power domain $\mathcal{U}_f\mathbf{X}$ coincide. They are explicitly given by

(1) $\mathcal{U}\mathbf{X} = \{K \subseteq \mathbf{X} \mid K$ is a Scott compact upper set$\}$ ordered by inverse inclusion '$\supseteq$',

(2) $\bigsqcup_{i \in I} A_i = \bigcap_{i \in I} A_i$ for directed families $(A_i)_{i \in I}$,

(3) $\theta = \emptyset$,

(4) $A \uplus B = A \cup B$,

(5) $\{\!|x|\!\} = \uparrow x$,

(6) $ext\, f\, A = \bigcup_{a \in A} fa = \bigcup f[A]$.

The initiality is indicated without proof in [10]. The finality of the construction in terms of compact sets is shown in [17] for sober domains — a much larger class of domains than the continuous ones. (Smyth naturally did not know our notion of finality at that time. He indicated a bijective correspondence between compact upper sets and 'open filters' proved in [11]. These open filters in turn bijectively correspond to our second order predicates $[[\mathbf{X} \to \mathbf{U}] \stackrel{rlin}{\to} \mathbf{U}]$.)

Unfortunately, the author does not know whether $\mathcal{U}_i\mathbf{X} = \mathcal{U}_f\mathbf{X}$ holds for all domains $\mathbf{X}$. Indeed, there is some evidence that it does not.[3] If so, *the* upper power domain does not exist — an ever lasting source of confusion.

10.3 Convex power constructions

Let $\mathbf{C} = \{0, 1\}$ with discrete order and $1 + 1 = 1$ be the *convex semiring*. $\mathbf{C}$-modules are just idempotent commutative monoids. Plotkin's power construction is known to be initial for this semiring as indicated in [10]. It much differs from the corresponding final construction $\mathcal{C}_f$.

If $\mathbf{X}$ is a domain with a least element $\perp$, then $[\mathbf{X} \to \mathbf{C}]$ has only two elements: $\lambda x.\, 0$ and $\lambda x.\, 1$. A linear second order function has to map $\lambda x.\, 0$ to 0. Thus, $\mathcal{C}_f\mathbf{X} = [[\mathbf{X} \to \mathbf{C}] \stackrel{rlin}{\to} \mathbf{C}]$ has two elements, no matter how big $\mathbf{X}$ is. Hence, $\mathcal{C}_f$ is quite useless.

Besides the initial and the final one, we know of nine further $\mathbf{C}$-constructions enumerated in [8].

10.4 Set domain constructions

As indicated in section 5.3, a power construction with a reasonable logic should have the Booleans as characteristic semiring. There are several semirings with carrier $\mathbf{B} = \{\perp, 0, 1\}$

[3] For topologists: $\mathcal{U}_i\mathbf{X}$ and $\mathcal{U}_f\mathbf{X}$ would differ for bounded complete, non-sober ground domains $\mathbf{X}$. I do not know whether such domains exist.

with $\perp \leq 0, 1$. In all of them, multiplication is given by parallel conjunction. Hence, we choose the semiring with addition being parallel disjunction. Power constructions with this characteristic semiring are called *set domain constructions* following [9]. They admit especially nice logical operations. Mixed power domain and sandwich power domain — defined for algebraic ground domains by Gunter and Buneman — provide two different set domain constructions.

The mixed power domain is free for the *mix theory* as Gunter [5, 6] and I independently found out. Mix algebras are commutative idempotent monoids enriched by an additional unary operation '?'.[4] In the following definition, we give — in contrast to Gunter — a minimal set of axioms, i.e. for each of the four axioms, there is a commutative idempotent monoid satisfying all axioms except the given one.

Definition 10.3 (Mix algebras)

A *mix algebra* $(\mathbf{P}, +, 0, \_?)$ is a commutative idempotent monoid domain $(\mathbf{P}, +, 0)$ with an additional continuous operation $\_? : \mathbf{P} \to \mathbf{P}$ satisfying the following 4 axioms

$$\begin{array}{llll} (A1) & A? \leq 0 & (A2) & A? \leq A \\ (A3) & A + A? \geq A & (A4) & (A+B)? \leq A? + B? \end{array}$$

A morphism f between two mix algebras is a mix homomorphism iff it is additive and satisfies $f(A?) = (fA)?$.

Mix algebras are nothing else than $\mathbf{B}$-modules; $A?$ is $\perp \cdot A$. The axioms of mix theory easily follow from the module axioms:

$$\begin{array}{ll} (I) & A + A = 1 \cdot A + 1 \cdot A = (1+1) \cdot A = 1 \cdot A = A \\ (A1) & A? = \perp \cdot A \leq 0 \cdot A = 0 \\ (A2) & A? = \perp \cdot A \leq 1 \cdot A = A \\ (A3) & A + A? = 1 \cdot A + \perp \cdot A = (1 + \perp) \cdot A = 1 \cdot A = A \\ (A4) & (A+B)? = \perp \cdot (A+B) = \perp \cdot A + \perp \cdot B = A? + B? \end{array}$$

The mix theory as defined above allows to derive some theorems which hold in all mix algebras. Among those, there is (A3) and (A4) with equality. We now present the most important of these theorems with their proofs which end up in a characterization of mix homomorphisms.

(T1) $A + B? \leq A$ since $A + B? \overset{A1}{\leq} A + 0 \overset{N}{=} A$

(T2) $A + A? = A$ by (A3) and (T1)

(T3) $0? = 0$ since $0 \overset{T2}{=} 0 + 0? \overset{N}{=} 0?$

(T4) $A?? = A?$ since $A?? \overset{A2}{\leq} A? \overset{T2}{=} A? + A?? \overset{T1}{\leq} A??$

(T5) $A? = A$ iff $A \leq 0$

Proof: '$\Rightarrow$' $A \overset{lhs}{=} A? \overset{A1}{\leq} 0$ '$\Leftarrow$' $A? \overset{A2}{\leq} A \overset{T2}{=} A + A? \overset{rhs}{\leq} 0 + A? \overset{N}{=} A?$

[4] denoted by $\Box$ by Gunter

(T6) $X \leq 0$ and $X \leq A$ iff $X \leq A?$ i.e. $A?$ is the greatest lower bound of 0 and A.
Proof: '$\Rightarrow$' $X \leq 0$ implies $X = X?$ by (T5). $X \leq A$ implies $X? \leq A?$ by monotonicity of '?'. Together, $X \leq A?$ follows. '$\Leftarrow$' by (A1) and (A2).

(T7) $(A + B)? = A? + B?$
Proof: '$\leq$' is (A4). '$\geq$' is deduced by (T6) from $A? + B? \leq 0$ (by (A1) and (N)) and $A? + B? \leq A + B$ (by (A2)).

(T8) The three statements $A \leq A + B$ and $A? \leq B?$ and $A? \leq B$ are equivalent.

$$\begin{aligned} \text{Proof}: \quad & (1) \Rightarrow (2): \quad A? \overset{1}{\leq} (A+B)? \overset{T7}{=} A? + B? \overset{T1}{\leq} B? \\ & (2) \Rightarrow (3): \quad A? \overset{2}{\leq} B? \overset{A2}{\leq} B \\ & (3) \Rightarrow (1): \quad A \overset{T2}{=} A + A? \overset{3}{\leq} A + B \end{aligned}$$

(T9) $X \leq 0$ and $X \leq A$ and $A + X \geq A$ iff $X = A?$
Proof: '$\Leftarrow$' is immediate by (A1), (A2), and (A3).
'$\Rightarrow$': $X \leq 0$ and $X \leq A$ imply $X \leq A?$ by (T6). $A + X \geq A$ implies $A? \leq X$ by (T8).

(T10) Every mix algebra is a **B**-module.

Proof: We define $0 \cdot A = 0$, $1 \cdot A = A$, and $\perp \cdot A = A?$. By (A1) and (A2), this operation is monotonic in its B-argument, whence it is continuous.

$r \cdot 0 = 0$:	(T3)
$r \cdot (A + B) = r \cdot A + r \cdot B$:	(T7)
$0 \cdot A = 0$:	immediate
$(r + s) \cdot A = r \cdot A + s \cdot A$:	by neutrality if $r = 0$ or $s = 0$, by idempotence if $r = s$, and by (T2) if $r = 1$ and $s = \perp$ or vice versa.
$1 \cdot A = A$:	immediate
$r \cdot (s \cdot A) = (r \cdot s) \cdot A$:	the only difficult case $r = s = \perp$ is handled by (T4).

Gunter defined mix algebras by an axiom system consisting of (T7), (T4), (T2), (A2), and (T1). Because (T1) implies (A1) by choosing $A = 0$ and (T2) implies (A3) and (T7) implies (A4), his mix theory is equivalent with ours.

(T9) is a particularly interesting theorem. It implies that the operation '?' is uniquely determined in a given mix algebra, i.e. for every commutative idempotent monoid, there is at most one choice for the operation '?' to turn it into a mix algebra. Another important consequence is the following:

Theorem 10.4

An additive morphism between two mix algebras is automatically a mix homomorphism, and an additive morphism between two **B**-modules is automatically linear.

Proof: Let $f : \mathbf{X} \to \mathbf{Y}$ be a continuous additive map between the two mix algebras $\mathbf{X}$ and $\mathbf{Y}$. Then for all $A \in \mathbf{X}$, $A? \leq 0$ and $A? \leq A$ and $A + A? \geq A$ imply $f(A?) \leq 0$ and $f(A?) \leq fA$ and $fA + f(A?) \geq fA$ respectively. By (T9), $f(A?) = (fA)?$ follows. □

Finally, one can show that the mixed power domain is initial for algebraic ground domain:

Theorem 10.5 For every algebraic domain $\mathbf{X}$, the mixed power domain over $\mathbf{X}$ and the initial set domain over $\mathbf{X}$ coincide.

A proof may be found in [5].

In contrast to the mixed power domain, the sandwich power domain is final:

Theorem 10.6 For every algebraic domain $\mathbf{X}$, the sandwich power domain over $\mathbf{X}$ and the final set domain $[[\mathbf{X} \to \mathbf{B}] \stackrel{rlin}{\to} \mathbf{B}]$ are isomorphic.

This theorem may be proven by combining the results about lower and upper power domain. A more clumsy, direct proof may be found in [7].

11 Conclusion

The algebraic framework introduced in this paper was developed to find out the common features of the known explicit constructions of Plotkin [14], Smyth [16, 17], Buneman et al. [2], and Gunter [5, 6]. It turned out to be general enough to cover also the proposals in [10, 12] concerning certain types of free monoids, and in [13] concerning free semiring modules.

The new notion of power homomorphisms immediately implies the notions of initiality and finality of power constructions. Whereas initiality is closely related to free modules, finality brings up a new aspect. The explicit description of final constructions in terms of second order 'predicates' indicates that such constructions may easily be implemented in a functional language that only has to provide the semiring addition as special feature (for the sandwich power domain for instance, this is 'parallel or').

The number of different power constructions satisfying the axioms of section 3 is enormous. For every semiring, there is an initial and a final construction that seem to coincide in rare cases only. Besides these two extremes, there might be a variety of other constructions with the same characteristic semiring. We found for instance nine further $\mathbf{C}$-constructions besides the initial and the final one. One might guess that the variety of different constructions increases with the complexity of the characteristic semiring.

The spectrum of power constructions with given characteristic semiring as well as the domain-theoretic properties of the initial and final construction are not yet thoroughly investigated (see the host of open problems indicated in this paper). Reasons might be the lack of examples and some inherent complexity of the theory. The five explicit constructions lower, upper, convex, mixed, and sandwich power domain have characteristic semirings of at most three elements, and even the seemingly simple case of the upper semiring is not completely understood (at least by the author).

A The core of an R-X-module

This appendix is concerned with the proof of Theorem 7.3 which characterizes the cores of R-$\mathbf{X}$-modules. The proof is not included in the main text because it uses topological methods instead of equational reasoning. As Theorem 7.3 is a generalization of some theorems in [12], many of the following auxiliary propositions may be found there. They are included here for the sake of completeness.

A.1 Directed closure

A subset S of a domain $\mathbf{X}$ is *directed closed* iff the suprema (w.r.t. $\mathbf{X}$) of all directed subsets of S belong to S. Since arbitrary intersections of directed closed subsets of $\mathbf{X}$ are directed closed, there is a least directed closed superset $\overline{A}$ for every subset A of $\mathbf{X}$. We show some properties of this set operator in the sequel.

Proposition A.1 If $f : \mathbf{X} \to \mathbf{Y}$ is a continuous function between two domains, then $f[\overline{A}] \subseteq \overline{f[A]}$ holds for all subsets A of $\mathbf{X}$.

Proof: Let $B = f^{-1}[\overline{f[A]}] = \{x \in \mathbf{X} \mid fx \in \overline{f[A]}\}$. For all a in A, $fa \in f[A] \subseteq \overline{f[A]}$ holds, whence $A \subseteq B$. If D is a directed subset of B, then $f[D]$ is a directed subset of $\overline{f[A]}$. $f(\bigsqcup D) = \bigsqcup f[D]$ holds by continuity of f. Since $\overline{f[A]}$ is directed closed, it contains $\bigsqcup f[D]$, whence $\bigsqcup D$ is in B.

Thus, we have seen that B is a directed closed superset of A. Hence, $\overline{A}$ is a subset of B, whence $f[\overline{A}] \subseteq \overline{f[A]}$. $\square$

Proposition A.2
Let $\mathbf{X}$ and $\mathbf{Y}$ be two domains, and $A \subseteq \mathbf{X}$ and $B \subseteq \mathbf{Y}$. Then $\overline{A \times B} = \overline{A} \times \overline{B}$ holds.

Proof: Let $\pi_1 : \mathbf{X} \times \mathbf{Y} \to \mathbf{X}$ and $\pi_2 : \mathbf{X} \times \mathbf{Y} \to \mathbf{Y}$ be the two projections. Since the projections are continuous, Prop. A.1 yields $\pi_1[\overline{A \times B}] \subseteq \overline{\pi_1[A \times B]} \subseteq \overline{A}$ and analogously $\pi_2[\overline{A \times B}] \subseteq \overline{B}$. These inclusions imply $\overline{A \times B} \subseteq \overline{A} \times \overline{B}$.

For the opposite direction, we also employ Prop. A.1. Using $\sigma_u = \lambda y.\,(u, y)$, one obtains for arbitrary sets $U \subseteq \mathbf{X}$ and $V \subseteq \mathbf{Y}$ the inclusion $U \times \overline{V} = \bigcup_{u \in U} \sigma_u[\overline{V}] \subseteq \bigcup_{u \in U} \overline{\sigma_u[V]} \subseteq \bigcup_{u \in U} \overline{U \times V} = \overline{U \times V}$. Analogously, one may show $\overline{U} \times V \subseteq \overline{U \times V}$. Combining both inclusions, one finally obtains $\overline{A} \times \overline{B} \subseteq \overline{A \times \overline{B}} \subseteq \overline{\overline{A \times B}} = \overline{A \times B}$. $\square$

The Proposition above allows to prove two statements about closure properties of sets w.r.t. continuous operations.

Proposition A.3 Let $\mathbf{X}$ be a domain and A a subset of $\mathbf{X}$.

(1) If A is closed w.r.t. a continuous unary operation $f : [\mathbf{X} \to \mathbf{X}]$, i.e. $f[A] \subseteq A$, then $\overline{A}$ is also closed w.r.t. f.

(2) If A is closed w.r.t. a continuous binary operation $g : [\mathbf{X} \times \mathbf{X} \to \mathbf{X}]$, i.e. $g[A \times A] \subseteq A$, then $\overline{A}$ is also closed w.r.t. g.

Proof:

(1) By Prop. A.1, $f[\overline{A}] \subseteq \overline{f[A]} \subseteq \overline{A}$ holds.

(2) By the same statement and Prop. A.2, we obtain $g[\overline{A} \times \overline{A}] = g[\overline{A \times A}] \subseteq \overline{g[A \times A]} \subseteq \overline{A}$. $\square$

Finally, we estimate the size of the directed closure.

Proposition A.4 Let A be a subset of a domain $\mathbf{X}$. Then $|\overline{A}| \leq 2^{|A|}$ holds.

Proof: Let $B = \{\bigsqcup S \mid S \subseteq A, \bigsqcup S \text{ exists}\}$. Then $A \subseteq B$ holds since $a = \bigsqcup\{a\}$ holds for all $a \in A$. We show that B is directed closed. If D is a directed subset of B, then for all d in D there is a subset S_d of A such that $d = \bigsqcup S_d$. Then $\bigsqcup D = \bigsqcup_{d \in D}(\bigsqcup S_d) = \bigsqcup(\bigcup_{d \in D} S_d)$. Because $\bigcup_{d \in D} S_d$ is a subset of A, $\bigsqcup D$ is a member of B.

Since B is a directed closed superset of A, $\overline{A} \subseteq B$ follows, whence $|\overline{A}| \leq |B| \leq |2^A| = 2^{|A|}$. □

Note that the set B in this proof contained the lubs of *all* subsets of A that exist, not only the lubs of the directed subsets of A. One might believe that the set $\widehat{A}$ of all lubs of *directed* subsets of A equals $\overline{A}$. This belief is however wrong; in general, $\widehat{A}$ does not contain the lubs of directed sets of lubs of directed sets of A.

A.2 Proof of Theorem 7.3

In this paragraph, the proof of Th. 7.3 is performed by means of some auxiliary propositions.

Proposition A.5 Let $\mathbf{M}$ be an R-$\mathbf{X}$-module. The set

$$\mathbf{M}^{\#} = \{r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n \mid n \in \mathbf{N}_0,\ r_i \in R,\ x_i \in \mathbf{X}\}$$

satisfies the properties (1) through (4) of Def. 7.2, i.e. $\mathbf{M}^{\#}$ contains 0 and all ηx, and is closed w.r.t. addition and multiplication by a factor in R.

Proof: Obvious. □

Proposition A.6 $|\mathbf{M}^{\#}| \leq |R|^{|\mathbf{X}|}$

Proof: Because of $r \cdot \eta x + r' \cdot \eta x = (r + r') \cdot \eta x$, one can arrange $r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n$ such that every x in $\mathbf{X}$ occurs at most once. Those x that do not occur may be added as $0 \cdot x$. Thus, $|\mathbf{M}^{\#}| \leq |\mathbf{X} \to R| = |R|^{|\mathbf{X}|}$. □

Proposition A.7 $\overline{\mathbf{M}^{\#}}$ satisfies properties (1) through (5) of Def. 7.2, i.e. it is an R-$\mathbf{X}$-submodule of $\mathbf{M}$.

Proof: (1) and (2) hold because of Prop. A.5 and $\mathbf{M}^{\#} \subseteq \overline{\mathbf{M}^{\#}}$. Property (3) for $\mathbf{M}^{\#}$ means this set is closed w.r.t. the binary continuous operation '+', whence $\overline{\mathbf{M}^{\#}}$ is also closed w.r.t. '+' by Prop. A.3 (2).

For $r \in R$, let $p_r : [M \to M]$ be given by $p_r\, m = r \cdot m$. Property (4) for $\mathbf{M}^{\#}$ means this set is closed w.r.t. the unary continuous operation p_r, whence $\overline{\mathbf{M}^{\#}}$ is also closed w.r.t. p_r by Prop. A.3 (1) for all r. □

Proposition A.8 $\mathbf{M}^c = \overline{\mathbf{M}^{\#}}$

Proof: By Prop. A.7, $\overline{\mathbf{M}^{\#}}$ is an R-$\mathbf{X}$-submodule of $\mathbf{M}$. Since $\mathbf{M}^c$ is the least such set, $\mathbf{M}^c \subseteq \overline{\mathbf{M}^{\#}}$ holds. Conversely, $\mathbf{M}^c$ being directed closed and $\mathbf{M}^{\#} \subseteq \mathbf{M}^c$ implies $\overline{\mathbf{M}^{\#}} \subseteq \mathbf{M}^c$.□

Proposition A.9 $|\mathbf{M}^c| \leq 2^{(|R|^{|\mathbf{X}|})}$

Proof: By Prop. A.6, $|\mathbf{M}^{\#}| \leq |R|^{|\mathbf{X}|}$ holds, and Prop. A.4 yields $|\overline{B}| \leq 2^{|B|}$. □

Acknowledgements

I am most grateful to Fritz Müller for his hints to the literature, many fruitful discussions, and suggestions on a draft version. Helmut Seidl also was always ready for discussions. Carl Gunter provided valuable hints to improve terminology and notation.

References

[1] M. Broy. A fixed point approach to applicative multiprogramming. In M. Broy and G. Schmidt, editors, *Theoretical Foundations of Programming Methodology.* Reidel, 1982.

[2] P. Buneman, S.B. Davidson, and A. Watters. A semantics for complex objects and approximate queries. Internal Report MS-CIS-87-99, University of Pennsylvania, October 1988. Also in: 7th ACM Principles of Database Systems.

[3] C.A. Gunter. Universal profinite domains. *Information and Computation*, 72:1–30, 1987.

[4] C.A. Gunter. A logical interpretation of powerdomains. Internal report without number and date, University of Pennsylvania, before September 1989.

[5] C.A. Gunter. The mixed powerdomain. Internal Report MS-CIS-89-77, Logic & Computation 18, University of Pennsylvania, December 1989.

[6] C.A. Gunter. Relating total and partial correctness interpretations of non-deterministic programs. In P. Hudak, editor, *Principles of Programming Languages (POPL '90)*, pages 306–319. ACM, 1990.

[7] R. Heckmann. Power domains and second order predicates. Study Note S.1.6-SN-25.0, Universität des Saarlandes, PROSPECTRA Project, February 1990.

[8] R. Heckmann. *Power Domain Constructions.* PhD thesis, Universität des Saarlandes, 1990.

[9] R. Heckmann. Set domains. In N. Jones, editor, *ESOP '90*, pages 177–196. *Lecture Notes in Computer Science 432*, Springer-Verlag, 1990.

[10] M.C.B Hennessy and G.D. Plotkin. Full abstraction for a simple parallel programming language. In J. Becvar, editor, *Foundations of Computer Science*, pages 108–120. *Lecture Notes in Computer Science 74*, Springer-Verlag, 1979.

[11] K. Hofmann and M. Mislove. Local compactness and continuous lattices. In Banaschewski and Hoffmann, editors, *Continuous Lattices, Bremen 1979. Lecture Notes in Mathematics 871*, Springer-Verlag, 1981.

[12] R. Hoofman. Powerdomains. Technical Report RUU-CS-87-23, Rijksuniversiteit Utrecht, November 1987.

[13] M.G. Main. Free constructions of powerdomains. In A. Melton, editor, *Mathematical Foundations of Programming Semantics*, pages 162–183. *Lecture Notes in Computer Science 239*, Springer-Verlag, 1985.

[14] G.D. Plotkin. A powerdomain construction. *SIAM Journal on Computing*, 5(3):452–487, 1976.

[15] M.B. Smyth and G.D. Plotkin. The category-theoretic solution of recursive domain equations. *SIAM Journal on Computing*, 11:761–783, 1982.

[16] M.B. Smyth. Power domains. *Journal of Computer and System Sciences*, 16:23–36, 1978.

[17] M.B. Smyth. Power domains and predicate transformers: A topological view. In J. Diaz, editor, *ICALP '83*, pages 662–676. *Lecture Notes in Computer Science 154*, Springer-Verlag, 1983.